Malware memory analysis of the IVYL Linux rootkit

Investigating a publicly available Linux rootkit using the Volatility memory analysis framework

Richard Carbone
EC-Council Certified Forensic Investigator (CHFI)
SANS GIAC Certified GCIH and GREM

DRDC – Valcartier Research Centre

Defence Research and Development Canada

Scientific Report
DRDC-RDDC-2015-R060
April 2015

IMPORTANT INFORMATIVE STATEMENTS

The content of this report is not advice and should not be treated as such.

Her Majesty the Queen in right of Canada, as represented by the Minister of National Defence ("Canada"), makes no representations or warranties, express or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this report. Moreover, nothing in this report should be interpreted as an endorsement of the specific use of any of the tools or techniques examined in it.

Any reliance on, or use of, any information, product, process or material included in this report is at the sole risk of the person so using it or relying on it.

Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this report.

Abstract

This report is the second in a series that will examine Linux Volatility-specific memory malware-based analysis techniques. Windows-based malware memory analysis techniques were analysed in a previous series. Unlike these Windows-based reports, some of the techniques described therein are not applicable to Linux-based analyses including data carving and anti-virus scanning. Thus, with minimal use of scanner-based technologies, the author will demonstrate what to look for while conducting Linux-specific Volatility-based investigations. Each investigation consists of an infected memory image and its accompanying Volatility memory profile that will be used to examine a different open source rootkit. Some of the rootkits are user-land while others are kernel-based. Rootkits were chosen over Trojans, worms and viruses as rootkits tend to be more sophisticated. This specific investigation examines the IVYL rootkit. It is hoped that through the proper application of various Volatility plugins combined with an in-depth knowledge of the Linux operating system, these case studies will provide guidance to other investigators in their own analyses.

Significance to defence and security

Canadian Armed Forces' (CAF) networks are a choice target for malware and directed attacks. This series of reports will provide junior and senior incident handlers alike with the necessary knowledge to investigate and mitigate complex attacks using only a memory image and a functional knowledge of the Linux operating system. As Linux continues to play a more important role in IT and the data centres of the Government of Canada and National Defence, some of these systems will invariably become infected. Thus, when this happens and when analysts and incident handlers have to intervene, it is hoped that these reports will have helped them to prepare for just such an occasion.

Résumé

Ce rapport est le second d'une série examinant les techniques spécifiques d'analyse de logiciels malveillants en mémoire sous Linux à l'aide de l'outil Volatility. Les techniques d'analyse de logiciels malveillants en mémoire pour Windows ont été décrites dans des rapports précédents. Cependant, certaines de ces techniques, telles que la récupération de données et le balayage d'antivirus ne s'appliquent pas aux analyses sous Linux. Par conséquent, avec une utilisation minimale des technologies de balayage, l'auteur démontrera ce qu'il faut rechercher lorsqu'on effectue des investigations spécifiques à Linux avec Volatility. Chaque investigation consiste en une image mémoire infectée, accompagnée de son profile mémoire Volatility, et examinera un programme malveillant furtif à code source ouvert différent. Certains seront en mode utilisateur tandis que d'autres seront en mode noyau. Les programmes malveillants furtifs ont été préférés aux chevaux de Troie, vers et virus, car ils ont tendance à être plus sophistiqués. La présente investigation examine spécifiquement le programme malveillant furtif IVYL. Il est espéré qu'avec une utilisation adéquate de différents plugiciels Volatility et d'une connaissance approfondie du système d'exploitation Linux, ces études de cas fourniront des conseils à d'autres enquêteurs pour leurs propres analyses.

Importance pour la défense et la sécurité

Les réseaux des Forces armées canadiennes (FAC) sont une cible de choix pour les logiciels malveillants et les attaques dirigées. Cette série de rapports fournira aux analystes en réponse aux incidents, aussi bien juniors que séniors, toute la connaissance requise pour investiguer et mitiger des attaques complexes en utilisant seulement une image de la mémoire et une connaissance fonctionnelle du système d'exploitation Linux. Comme Linux joue un rôle de plus en plus important dans les TI et les centres de données du gouvernement du Canada et de la Défense nationale, certains de ces systèmes deviendront invariablement infectés. Par conséquent, quand cela arrivera et que des analystes en réponses aux incidents auront à intervenir, nous espérons que ces rapports les auront aidés à se préparer à une telle occasion.

Table of contents

List of figures

List of tables

Acknowledgements

The author would like to thank Mr. Francois Rheaume, Defence Scientist, for conducting both a preliminary and peer review of this text as well as providing helpful comments in order to improve it. Moreover, the author would also like to extend his thanks to Mr. Martin Salois, Defence Scientist, for helping to make major improvements to text and to Philippe Charland, Defence Scientist, for translating portions of this text.

Disclaimer policy

It must be understood from the outset that this report examines computer malware and that handling virulent software is not without risk. As such, the reader should ensure that he has taken all the necessary precautions to avoid infecting his own computer system and those around him, whether on a corporate network or isolated system.

The reader must neither construe nor interpret the work described herein by the author as an endorsement of the aforementioned techniques and capacities as suitable for any specific purpose, construed, implied or otherwise. Moreover, the author does not endorse the specific use of any of the tools or techniques examined herein. While the author felt most comfortable working from within a Linux environment, the author does not specifically recommend the use of such a system for the reader. Instead, the reader should use the environment in which he is most comfortable.

Furthermore, the author of this report absolves himself in all ways conceivable with respect to how the reader may use, interpret or construe this report. The author assumes absolutely no liability or responsibility, implied or explicit. Moreover, the onus is on the reader to be appropriately equipped and knowledgeable in the application of digital forensics. Due to the offensive nature of computer malware, the author is no way responsible for the reader's use of any malware, whether examined herein or otherwise, in any offensive or defensive nature against any entity, even against the reader himself, for any purpose whatsoever.

Finally, the author and the Government of Canada are henceforth absolved from all wrongdoing, whether intentional, unintentional, construed or misunderstood on the part of the reader. If the reader does not agree to these terms, then his copy of this Scientific Report must be destroyed. Only if the reader agrees to these terms should he continue in reading it beyond this point. It is further assumed by all participants that if the reader has not read said Disclaimer upon reading this report and has acted upon its contents then the reader assumes all responsibility for any repercussions that may result from the information and data contained herein.

Requirements, assumptions and exclusions

The author assumes that the reader is altogether familiar with digital forensics and the various techniques and methodologies associated therein. This report is not an introduction to digital forensics or to said techniques and methodologies. However, the author has endeavoured to ensure that the reader can carry out his own forensic analysis of a computer memory image suspected of malware infection based on the information and techniques described herein.

The experimentation conducted throughout this report was carried out atop a Fedora 21 64-bit Linux operating system. Unlike the various Windows infected memory case studies, neither anti-virus (AV) nor data carving techniques worked particularly well against Linux-based memory images. As such, the former is used minimally while the latter is not at all used in this report. Consequently, the methodology presented in this series of reports is quite different from that presented in the Windows Volatility-based series of memory malware analyses.

It is important that the reader have permission to use these tools on his computer system or network. Use of these tools and the analysis of virulent software always carry some inherent risk that must be securely managed and adequately mitigated.

An in-depth study of memory analysis techniques is outside the scope of this work, as it requires a comprehensive study of operating system internals and software reverse engineering techniques, both of which are difficult subjects to approach. Instead, this work should be considered as a guide to using the Volatility memory analysis framework for the analysis of a Linux-based memory malware infection.

In this report, the use of the words rootkit, infection and malware are used interchangeably. The same applies for kernel module, driver and Loadable Kernel Modules (LKM).

Finally, the use of masculine is employed throughout this text for the purpose of simplification.

Availability of Linux memory images and profiles

Various Linux-based memory images are available from different publicly available sources, most notably among them those from SecondLook. The author, for the time being, has endeavoured to build his own virtual machines and memory profiles to be independent of those already available.

The author will endeavour to ensure that his memory images and profiles will be made available to anyone requesting a copy, as laws and international agreements allow. The author can be contacted at val-forensics@drdc-rddc.gc.ca. Please state your name, organization, country and mailing address including additional contact information and one will be mailed to you within a reasonable delay. No PO Boxes will be accepted—commercial and government mailing addresses only.

This page intentionally left blank.

1 Background

1.1 Objective

The objective of this report is to examine how a computer forensic investigator/incident handler, without specialised computer memory or software reverse engineering skills, can successfully investigate a Linux-based memory image suspected of infection.

To successfully investigate such an image, this report will use an applied plugin-based approach as it uses demonstrable procedures that intermediate-level investigators and incident handlers can use as a basis for investigating suspected memory images.

The work is based on the publicly available source code for the IVYL rootkit. This document is the third in a series of reports that examines Linux-based malware memory analysis. This specific report surveys what to look for when examining a kernel-based rootkit. Ultimately, these reports will provide a foundational framework that novice and experienced investigators alike can rely on for guidance when investigating infected Linux memory images.

Unlike the previous Windows-based reports, it was determined that Linux-specific memory analysis case studies and reports have been left woefully unexamined by the community, at least as of the time of this writing, hence prompting the author to write this case study and its subsequent follow-up studies.

1.2 Project support

This work was carried out over a period of several months as a collaborative effort between DRDC – Valcartier Research Centre and the RCMP, as part of the Live Computer Forensics project (SRE-09-015, 31XF20).

1.3 Target audience

The results of this project may also be of great interest to the Canadian Forces Network Operations Centre (CFNOC), the RCMP's Integrated Technological Crime Unit (ITCU), the Sûreté du Québec and other law enforcement-related cyber investigation teams.

The target audience for this report is the computer forensic investigator who assesses suspect computer memory images for evidence of infection and the incident handler who is called on to assess or intervene in a possible malware infection. While previous reports were targeted at investigators and incident handlers working with Windows-based memory images and malware, this new series of reports will be directed at those who must analyse Linux malware-infected memory images.

The skills amassed by incident handlers and investigators alike while using Volatility to examine Windows memory images will be of some help. However, Linux and Windows are not the same and while there is commonality in the approach used by the author throughout both series of

reports, important differences are apparent. To extract the maximum value from this report, the reader should have a working knowledge of Linux, basic system administration and software compilation.

1.4 IVYL rootkit background

Written by Arkadiusz Hiler (ivyl) and t3hknr, IVYL is a kernel-based rootkit. While it does have some useful capabilities that some will find interesting, it does not have the ability to perform Pluggable Authentication Module (PAM) hooking nor does it provide for a configuration file for enabling specific functionality prior to compilation, unlike KBeast [8].

As is somewhat common with anti-virus (AV) vendors, no technical analysis was available from them concerning IVYL. What is known about it comes from information made available by its author. The source code was accompanied by a more technical document that was unfortunately only available in Polish. The version of the rootkit's source code used in this analysis is the latest version, released October 2013.

IVYL is a kernel rootkit and must be compiled and loaded into kernel-space to infect the system. Since there is no supplemental configuration file, compilation is straightforward, relying exclusively on the included Makefile for compilation. However, to load the rootkit Loadable Kernel Module (LKM), the attacker must have already gained root-level access.

According to the rootkit's author, it is a "sample" rootkit with the following capabilities [1, 2]:

- Creates kernel */proc* structure */proc/rtkit* from which to issue rootkit-specific commands;
- Has the ability to hide (remove itself from the list of modules);
- File hiding (achieved by hooking *procfs* and *readdir* calls);
- Ability to open a root shell; and
- Ability to change memory page rights.

Based on this list of capabilities, it does not appear to be as advanced as KBeast or Jynx2 [8, 9]. However, as this analysis will reveal, this rootkit is very difficult to identify by itself in so long as no augmented root shell has been opened. Even so, this rootkit could be easily augmented due to its open source nature.

A brief analysis of the source code indicates that these capabilities appear to be valid claims; however, the author has not verified them in-depth. Nevertheless, there is no reason to believe these claims to be false. Moreover, insufficient information is available to determine which kernels the rootkit is capable of infecting. Finally, rootkit compilation specifics are found in Section 1.6.

1.5 Information concerning the guest VM

The Linux test virtual machine (VM) which was infected with IVYL was built atop Ubuntu 11.04 x64 and was installed from DVD media. The VM was allocated 2 CPUs and 4 GiB RAM and the

default Ubuntu VirtualBox parameters for the VM were used. Once the VM's operating system was installed and found to be functional, VirtualBox's Guest Additions were installed. The system appeared to be in good working order except that *dwarfdump* and its required dependencies were not installed from the DVD media installation and the various online repositories for Ubuntu 11.04 were no longer available. Thus, the source code for the variously required packages had to be downloaded from the web, compiled and then installed within the VM. Once this was done, the operating system was then temporarily shut down.

1.6 Compiling and loading the rootkit

The rootkit's source code, found in downloaded file *rootkit-master.zip* (SHA1 hash of DA750D4DB065480CC6243C34A55EDD7E901CE63B), was copied over to the VM through a *shared folder* (mounted read-only) atop directory */tmp,* where it was unpackaged and compiled according to the following commands:

```
$       mkdir /rootkit

$       mv rootkit-master.zip /rootkit; cd /rootkit

$       unzip rootkit-master.zip

$       make
```

Upon successful compilation, the rootkit is then loaded by the attacker into kernel-space using command *insmod rt.ko*. The rootkit is now compiled and loaded.

To obtain a list of commands available from the rootkit, use command *cat /proc/rtkit*. To gain a root shell, use the shell program *tools/rtcmd.py* found within the tools directory where the rootkit's ZIP archive was unpacked and type *tools/rtcmd.py mypenislong*[1] */bin/bash*.

[1] My Pen Is Long.

Available commands for this particular version of the rootkit are shown in the following figure:

```
RTKIT
DESC:
  hides files prefixed with __rt or 10-__rt and gives root
CMNDS:
  mypenislong - uid and gid 0 for writing process
  hpXXXX - hides proc with id XXXX
  up - unhides last process
  thf - toogles file hiding
  mh - module hide
  ms - module show
STATUS
  fshide: 1
  pids_hidden: 0
  module_hidden: 1
```

***Figure 1**: Command output for cat /proc/rtkit.*

Running *tools/rtcmd.py* results in a command shell, regardless of the user's UID. */proc/rtkit* is not visible to the system when perusing */proc*; its existence must be known, as its presence cannot be derived by looking at the files in this directory.

1.7 Memory image metadata

Two memory images were taken of the VM. One was taken just prior to infection and the other just after rootkit infection. In so doing, it is possible to compare a clean system to an infected system in the event that such comparative information is required during the analysis of the infected memory image.

For these two memory images, similarities in their fuzzy hashes have been identified in Table 1 and Table 2 below (pink characters) to identify large memory structures that have more or less remained the same [13].

Both acquired memory images should have been exactly 4 GiB in size, but as it turned out were not. Instead, they were each approximately 3% larger, thereby indicating that the VirtualBox-specific overhead for this memory dump was non-negligible.

The VM's memory was dumped to obtain an uninfected baseline memory. This was done by restarting the VM using the following command [3]:

```
$ virtualbox --debug --startvm "Ubuntu 11.04 x64"
```

VM memory was then dumped using the following command [3]:

```
$ vboxmanage debugvm "Ubuntu 11.04 x64" dumpguestcore --filename
  ubuntu11_04_IVYL.mem
```

This process was repeated shortly after infection of the VM.

The Volatility profile, *ubuntu_1104_x64_profile.zip*, was generated as per the instructions found in [7]. The profile is available to the reader as per the eligibility requirements set out on *page xiii*.

1.7.1 Uninfected baseline memory image metadata

The metadata in Table 1 accurately describes the uninfected baseline memory image.

***Table 1**: Linux Ubuntu 11.04 x64 uninfected memory image metadata.*

Memory image name	ubuntu_1104_base.mem
Actual size (exact)	4,433,464,300 bytes
Expected size (exact)	4,294,967,296 bytes
SHA1 hash	2418140bbf0bbc127060e1e88dd2b1ebed9ff5fc
Fuzzy hash	1572864:+KPyCJuc0VVMRdoe0kVx8wQzdB5YpQVHQ9zrqaIIBUu QQBm32+uzQjn6I32H+x9:fyCkct2zerQIBUDQB82+YsivjKRP1y

1.7.2 Infected memory image metadata

The metadata in Table 2 accurately describes the infected memory image.

***Table 2**: Linux Ubuntu 11.04 x64 IVYL infected memory image metadata.*

Memory image name	ubuntu_1104_IVYL.mem
Actual size (exact)	4,433,464,300 bytes
Expected size (exact)	4,294,967,296 bytes
SHA1 hash	27776a171bd8ea55826d6cecb8c1feee7a2ca94b
Fuzzy hash	3145728:RyCksLpf27G6r9IBmZ7Jo3C3FV4zEogszf+m:dLpf27fr9IB mjwR

1.8 AV scanners used

This report makes use of six anti-virus scanners, the same six as those used in reports [8, 9]. These scanners continue to represent a wide cross-section of various detection mechanisms necessary for the detection of diverse malware. Each scanner was updated December 2, 2014; the analysis was then carried out. Scanner specifics are listed in Table 3.

***Table 3**: List of anti-virus scanners and their command line parameters.*

Anti-virus scanner	Command line parameters
Avast v.1.3.0 command line scanner	avast -c
AVG 2013 command line scanner version 13.0.3114	avgscan -H -P -p
BitDefender for Unices v7.90123 Linux-amd64 scanner command line	bdscan (no parameters used)
Comodo Antivirus Product Version 1.1.268025.1 / Virus Signature Database Version 16954	cmdscan -v -s
FRISK F-Prot version 6.3.3.5015 command line scanner	fpscan -u 4 -s 4 -z 10 --adware --applications --nospin
McAfee VirusScan for Linux64 Version 6.0.3.356 command line scanner	uvscan --RECURSIVE --ANALYZE --MANALYZE --MIME --PANALYZE --UNZIP --VERBOSE

2 Peripheral concerns

2.1 Why examine Linux memory images or make them available?

After extensively searching the available public literature, it became clear that few detailed Linux-based memory analyses could be found. In addition, those few reports or documents that were found were not of sufficient quality to enable others to readily learn the necessary techniques or approaches to conducting their own analyses that were specifically targeted towards non-memory specialists and non-reverse engineers. The author has opted to build his own virtual machines and infect them to be independent of those already done.

The author asserts that by methodically conducting various Linux-based memory analyses using a memory analysis framework such as Volatility and sharing the techniques and methods used for these analyses with the digital forensics community, it will help to further advance the capabilities of investigators and incident handlers alike when dealing with potentially infected Linux memory images. Just as with the now completed Windows series of reports, which provide a detailed methodology for conducting Volatility-based malware memory analysis for non-experts, this series of Linux-based reports hope to have the same impact for the Linux audience.

2.2 Volatility background

Volatility 2.4 is used for the analysis of the memory image infected by the IVYL rootkit. The version of this framework, at the time of writing, is considered the stable public release and is suitable for use by both the general public and investigators alike, although it may not necessarily have the most recent or bleeding-edge plugins. It was released for public use August 2014.

Originally written by Aaron Walters of Volatile Systems, Volatility has become a full-fledged memory analysis framework. It is written entirely in Python and can therefore be run atop Windows, Linux and other various operating systems supporting Python. Volatility began supporting Linux-based memory analysis in previous versions, although its current support has improved a great deal. However, its Windows support continues to remain both more robust and reliable. Currently, it is developed by a variety of contributors, although the most well-known of these are Michael Ligh, Jamie Levy, Brendan Dolan-Gavitt, Andrew Case and Mike Auty. Furthermore, each of these individuals has made significant contributions to the digital forensics community over the last few years. Michael Cohen, who was formerly with the project, has gone on to found *Rekall* (https://code.google.com/p/rekall), a memory analysis framework similar to Volatility that at the time of this writing is not yet ready for public use.

The Linux plugins supported by version 2.4 of Volatility are described in Annex A.

2.3 Purpose of these tutorials

Although online tutorials concerning infected Linux-based memory images exist, these tutorials are generally written for a highly technical audience already familiar with software reverse

engineering and memory forensics. They typically provide either too little information or are too technical to be of much use to most investigators and incident handlers.

Thus, the author asserts that by re-examining and thoroughly documenting the steps and procedures used to identify various rootkit-based infections will aid the reader in unravelling his own malware-based investigations. It is hoped that these reports will build a compendium of knowledge to serve the forensic community as learning guides and tutorials.

The author has made all efforts to ensure that this document and the investigation of the IVYL rootkit are comprehensible to the general computer forensic practitioner, in the hopes of reaching as wide an audience as possible and having a more significant impact.

2.4 Issues concerning data carving

Unlike Windows-based memory images, it turns out that data carving is not particularly effective against Linux-based memory images. Experimentation by the author has revealed that once a Linux binary, whether an executable or a compiled library file, has been loaded into memory, it loses its ELF header, thereby making its detection and subsequent carving very difficult. Without an ELF header from which to start, data carvers and recovery software will not be able to identify the starting point of a given library or executable in memory. The author attempted ten different memory experiments using both 32 and 64-bit Linux operating systems. Between them, only one ELF-based file was ever recovered. The other files recovered were mostly text-based data files.

The reader may recall that these same data carving techniques worked moderately well against Windows-based memory images. This is because Windows executables and libraries have their PE header loaded into memory, making them readily identifiable and recoverable.

Moreover, the various techniques examined in the Windows series of reports found that occasionally some of the malware carved from a memory image matched those dumped from the memory image using Volatility. What this means is that data recovery tools and software are more likely to recover intact (or partially intact) malware from Windows memory images as compared to those from Linux. The various MD5/SHA1 and fuzzy hashing (file similarity matching) used for Windows also confirms this assertion. As of Volatility 2.4, a new plugin, *linux_elf*, has been designed to help investigators determine where ELF files are residing within a memory image using alternate means.

2.5 Issues concerning AV analysis

Further complicating Linux-based malware memory analysis is the lack of Linux-specific malware detection using various AV scanners. While the various scanners used throughout the Windows reports worked well against both Volatility-dumped and data-carved files, these very same AV scanners (Avast, AVG, BitDefender, ClamAV[2], Comodo[2], Frisk F-Prot and McAfee) fared poorly against the Linux-based rootkits. Quite the opposite was in fact expected. Since these rootkits were all open source, it would have followed that the various scanners would have

[2] This AV was used in some Windows memory malware reports but not others.

included some basic signature or heuristic detection capability. After all, these rootkits will inevitably be used as the basis for future rootkits. Unfortunately, this was not the case at all.

Thus, both this report and the series of Linux-based reports will make little use of AV scanners. That, however, requires the reader to have a very good understanding of Linux to make up for what the scanners fail to detect. Nevertheless, certain portions of each Linux-based report will still use AV scanners in the hope that they may be able to reveal something pertinent concerning a rootkit. Specifics are available in the analysis portion of this and subsequent follow-up reports.

2.6 Issues concerning the NSRL

The National Software Reference Library (NSRL) is a standardised and trustworthy source of computer operating system and application file names and hashes (MD5/SHA1). It is not particularly well suited to Linux-based investigations as there are far too many Linux distributions (hundreds of publicly available distributions are known to exist) to be covered by the NSRL, including all the various kernel versions in use[3]. As such, it does not make sense to rely on the NSRL for file name listings and hashes for comparative purposes against data files recovered from a Linux memory image. For that reason, these reports and their examination of various infected Linux memory images will not use the NSRL as was done for the Windows series of reports.

[3] A full listing of which Linux distributions are supported by a given version of the NSRL can be found in its "*nsrlprod.txt*" file.

3 Memory analysis of IVYL using Volatility

3.1 Step 1: AV analysis of memory images and source code

This step examines an infected memory image, source code and compiled rootkit using the various scanners in the hope of identifying any of them as infected.

3.1.1 Memory image analysis

None of the scanners listed in Section 1.8 found anything in memory image *ubuntu_1104_IVYL.mem*.

3.1.2 Rootkit analysis

The compiled rootkit, file *rt.ko*, was obtained by manually mounting the VM disk image and copying it to the host system's disk. This file was then scanned where nothing was detected.

This file is 11,998 bytes in size with a SHA1 hash of 0BE6D9510737EC6D96A361B53CA0C22CCAEC1529. It was submitted to VirusTotal[4] for inspection against a total of 57 scanners, all of which failed to detect anything.

3.2 Step 2: Volatility system information extraction

This next step examines the infected memory image using Volatility plugins that provide system information about the suspect computer and its operating system.

3.2.1 Plugin linux_banner

This plugin is used to determine the Linux kernel, its revision and architecture. The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_banner
```

The plugin generated the following output:

```
Linux version 2.6.38-8-generic (buildd@allspice) (gcc version 4.5.2
(Ubuntu/Linaro 4.5.2-8ubuntu3) ) #42-Ubuntu SMP Mon Apr 11 03:31:24 UTC
2011 (Ubuntu 2.6.38-8.42-generic 2.6.38.2)
```

[4] More information concerning the submission of this particular rootkit can be found at https://www.virustotal.com/en/file/9bf9889168b5d9d776c35d7180ece78615183402b412e6ca227f3e1b042a7db0/analysis/.

The output indicates that Linux 2.6.38-8 is running and that it is an SMP-enabled kernel, compiled using GCC version 4.5.2 (April 11, 2011). However, looking only at this information it is not possible to determine if it is a 32-bit, 32-bit PAE or 64-bit kernel. To be fair, part of the problem is the kernel naming convention used by Debian and Ubuntu, in this case, for example, Ubuntu 2.6.38-8.42-generic 2.6.38.2.

3.2.2 Plugin linux_cpuinfo

This plugin is used to identify the type and number of CPUs running atop the suspect computer. The plugin was run using the following command resulting in the following output:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_cpuinfo
Processor   Vendor          Model
----------  ----------------    ------------------------------------------------------------
0           GenuineIntel    Intel(R) Core(TM) i7 CPU     X 000  @ 3.33GHz
1           GenuineIntel    Intel(R) Core(TM) i7 CPU     X 000  @ 3.33GHz
```

The make and model of the two identified processors are correct. The base processor speed is 3.33 GHz.

3.2.3 Plugin linux_dmesg

This plugin is used to identify important boot-up information and kernel-based messages about the underlying computer system. The UNIX/Linux *dmesg* command, upon which this plugin is based, identifies various kernel and device driver boot-up information and output structures in memory that are typically found in system log file */var/log/dmesg*[5].

Using this plugin, it may be possible to identify what kernel (and its revision) was running, the number and type of CPUs, instantiated system services, the map of system memory, networking and many other essential capabilities (both software and hardware) that a typical Linux system will have. The plugin was run using the following command:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_dmesg
```

The output is too long to list here, but a full listing can be found in Annex B.1. After a detailed inspection of the output, nothing out of the ordinary was identified.

[5] Not all UNIX systems necessarily use this specific file. Mileage will vary according to the underlying operating system.

3.2.4 Plugin linux_iomem

This plugin provides the physical memory mapping of the suspect computer system, which in this case is a virtual machine. An in-depth examination of this virtual machine's physical memory mapping is outside the scope of this report; however, additional information concerning the interpretation of this data can be found in [4].

The plugin was run using the following command:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_iomem
```

The output of this plugin is listed in the first three columns of Table 4. The fourth and fifth columns were added by the author to facilitate reading. In blue, we find the virtualized hardware RAM (equivalent to computer hardware memory modules).

***Table 4**: VM physical memory mapping for suspected system.*

Hardware	Starting Address	Ending Address	Size Difference	Size (in bytes)
reserved	0x0	0xFFFF	0xFFFF	65,536
System RAM	**0x10000**	**0x9FBFF**	**0x8FBFF**	**588,800**
reserved	0x9FC00	0x9FFFF	0x3FF	1,024
reserved	0xF0000	0xFFFFF	0xFFFF	65,536
System RAM	**0x100000**	**0xDFFEFFFF**	**0xDFEEFFFF**	**3,756,982,272**
Kernel code	0x1000000	0x15CD2BC	0x5CD2BC	6,083,260
Kernel data	0x15CD2BD	0x1AB38FF	0x4E6642	5,137,986
Kernel bss	0x1BAA000	0x1CFEFFF	0x731D42	7,544,130
ACPI Tables	0xDFFF0000	0xDFFFFFFF	0xFFFF	65,536
0000:00:02.0	0xE0000000	0xE7FFFFFF	0x7FFFFFF	13,4217,728
vesafb	0xE0000000	0xE012FFFF	0x12FFFF	1,245,184
0000:00:03.0	0xF0000000	0xF001FFFF	0x1FFFF	131,072
e1000	0xF0000000	0xF001FFFF	0x1FFFF	131,072
0000:00:04.0	0xF0400000	0xF07FFFFF	0x3FFFFF	4,194,304
vboxguest	0xF0400000	0xF07FFFFF	0x3FFFFF	4,194,304
0000:00:04.0	0xF0800000	0xF0803FFF	0x3FFF	16,384
0000:00:06.0	0xF0804000	0xF0804FFF	0xFFF	4,096
ohci_hcd	0xF0804000	0xF0804FFF	0xFFF	4,096
0000:00:0b.0	0xF0805000	0xF0805FFF	0xFFF	4,096
ehci_hcd	0xF0805000	0xF0805FFF	0xFFF	4,096
0000:00:0d.0	0xF0806000	0xF0807FFF	0x1FFF	8,192
ahci	0xF0806000	0xF0807FFF	0x1FFF	8,192
IOAPIC 0	0xFEC00000	0xFEC003FF	0x3FF	1,024
Local APIC	0xFEE00000	0xFEE00FFF	0xFFF	4,096

Hardware	Starting Address	Ending Address	Size Difference	Size (in bytes)
reserved	0xFFFC0000	0xFFFFFFFF	0x3FFFF	262,144
System RAM	**0x100000000**	**0x11FFFFFFF**	**0x1FFFFFFF**	**536,870,912**

The VM, allocated a total of 4,294,967,296 bytes (4 GiB) RAM is able to use 4,294,441,984 bytes, leaving 525,312 (513 KiB) bytes left reserved for use by the VM's BIOS.

The reason an investigator/incident handler should use this plugin is to be aware of the different address ranges used by the hardware (virtualized or not) and operating system. This information can be used to validate that the malware has not tricked the operating system's virtual memory manager or other kernel components into thinking the system has less memory than it physically has. Had the amount of unseen memory been significantly larger than the 509 KiB used by the BIOS, then this could have indicated that the malware was busy making changes to the system to hide itself. While this capability has not yet been seen in Linux malware, this does not preclude it from existing.

3.2.5 Plugin linux_slabinfo

Plugin *linux_slabinfo* is used to provide kernel SLAB-based information. The kernel SLAB structure is a specific structure kept in */proc* used to keep track of the different kernel structures that rely on various caches. These include, but are not limited to filesystem buffers, network buffers and caches, inodes and many others.

This plugin only supports SLAB-based kernels and as such will only work with memory images using kernel 2.6.22 and earlier. Kernels 2.6.23 and later, by default, use SLUB-based memory management [4, 5, 6].

3.2.6 Plugin linux_mount_cache

Plugin *linux_mount_cache* is used to provide kernel SLAB-based information. The kernel SLAB structure is a specific structure kept in */proc* used to keep track of different kernel structures that rely on various caches. These include, but are not limited to, filesystem buffers, network buffers and caches, inodes and many others.

The reason this plugin does not work is that it supports SLAB-only based kernels, not SLUB-based kernels [4, 5, 6].

3.2.7 Plugin linux_mount

Although this plugin is not the preferred manner for obtaining a list of mounted disk, kernel and virtual filesystems, it did work, unlike the previous plugin, even if some of the output is not the same as what the *linux_mount_cache* plugin would produce.

The plugin was run using the following command generating the following output:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_mount
```

- ---------- /media/malware vboxsf rw,relatime,nodev
- /dev/sda1 /boot ext4 rw,relatime
- /dev/disk/by-uuid/45fdcb1c-c3c7-4c98-9ac3-7f8acf84ac26 / xfs rw,relatime
- binfmt_misc /proc/sys/fs/binfmt_misc binfmt_misc rw,relatime,nosuid,nodev,noexec
- fusectl /sys/fs/fuse/connections fusectl rw,relatime
- gvfs-fuse-daemon /home/richard/.gvfs fuse rw,relatime,nosuid,nodev
- none /var/run tmpfs rw,relatime,nosuid
- none /sys/kernel/debug debugfs rw,relatime
- none /sys sysfs rw,relatime,nosuid,nodev,noexec
- none /dev/shm tmpfs rw,relatime,nosuid,nodev
- none /dev devtmpfs rw,relatime
- none /var/lock tmpfs rw,relatime,nosuid,nodev,noexec
- none /proc proc rw,relatime,nosuid,nodev,noexec
- none /dev/pts devpts rw,relatime,nosuid,noexec
- none /sys/kernel/security securityfs rw,relatime

The first entry is the VirtualBox Shared Folder that was mounted on the guest VM. That aside, upon closer examination of the output, nothing appears out of the ordinary.

3.2.8 Summary

Performing Volatility system information extraction has demonstrated that collecting information about the VM's underlying operating system and base configuration is straightforward. However, despite the many pages of output generated by the various plugins, no clues or hints as to this memory image's infection could be identified.

These plugins do provide important basic information about the underlying hardware and operating system, which, while informative, are unlikely to yield immediate clues. Upon correlation with additional plugins (yet to be used), they may yield further information.

The author is of the opinion that the most important plugin in this step is *linux_dmesg*. However, plugins *linux_iomem* and *linux_mount* may provide additional indications of malware presence, but only if the malware is capable of modifying the kernel's perception of available "System

RAM" or mount points, respectively. Plugin *linux_banner* is useful for obtaining information about the version of the kernel in use but on its own provides no information about the architecture of the kernel (32 or 64-bit).

It is important that analysts use the appropriate Volatility plugins supported by the memory image's underlying kernel and recognize which is SLUB and SLAB based. That is the reason why the author continues to use them even though they will not work against more recent versions of the Linux kernel.

3.3 Step 3: Volatility process listings and analysis

In this step, specific plugins will be used to identify process-based information concerning the infected memory image.

3.3.1 Plugin linux_psaux

This plugin is used to provide a full process listing of the system. Its output is approximately the same as would be obtained running the *ps -aux* command via a terminal. The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
  ubuntu_1104_IVYL.mem linux_psaux
```

The resulting output consisted of 146 listed processes. This output is too long to list here, but it can be found in Annex B.2. Everything in this long list of processes appears altogether normal.

3.3.2 Plugin linux_pslist

This interesting Volatility plugin is also used to list all running processes on a system. It works by walking the *task_struct->tasks* linked list [10, 12], similar to Volatility's Windows process listing plugins. The plugin can list all active processes (except for the system swapping process(es)). According to Volatility's documentation, if the output under the DTB column is blank then it is very likely a kernel thread. This includes drivers and other kernel modules visible from userland.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
  ubuntu_1104_IVYL.mem linux_pslist
```

The resulting output is too long to include here but can be found in Annex B.3. Importantly, the same numbers of processes (146) were found using this plugin as with the previous plugin. Again, nothing out of the ordinary was identified.

3.3.3 Plugin linux_pslist_cache

This plugin attempts to build a list of active processes from *kmem_cache*, the kernel's memory cache [10, 12]. In effect, it should reproduce the same results as the *linux_pslist* plugin using a different mechanism, which is useful in corroborating the results of the other available process listing plugins.

The reason this plugin does not work is that it supports SLAB-only based kernels, not SLUB-based kernels [4, 5, 6].

3.3.4 Plugin linux_pstree

The purpose of this plugin is to identify the relationship between processes, in effect to identify a given process' parent (or PPID). The reader may have noticed that to date none of the Linux process listing plugins provides the PPID of the variously identified processes. Thus, to identify these relationships, the following command was issued:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_pstree
```

The resulting output is too long to include here but can be found in Annex B.4. Importantly, the same numbers of processes (146) were found using this plugin as with the previous plugin. Again, nothing out of the ordinary was identified.

3.3.5 Plugin linux_pidhashtable

This interesting plugin can be used to identify hidden or previously unseen processes. However, it is not the same as the Windows *psxview* plugin. Instead, it works by walking the PID hash table [10, 12]. The *plugin* validates that a given process forms part of the PID hash table maintained by the operating system. This lookup (or hash) table is similar to that used by Windows in that they are both doubly linked lists. In the same manner that rogue Windows processes can unlink themselves from the Windows process table, rogue Linux processes can unlink themselves from the PID hash table and this plugin can aid in identifying them. Its output is not that different from the *linux_pslist* plugin.

The plugin was run using the following command:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_pidhashtable
```

The resulting output is too long to include here but can be found in Annex B.5. Nearly double the numbers of processes (276) were found using this plugin. Interestingly, the very last line of output found in this table had a suspicious looking entry, found listed below in Table 5.

***Table 5**: Identification of a possibly suspicious process using plugin linux_pidhashtable.*

Offset	0xffff8801156788b8
Name	?GQ???
Pid	2800
Uid	1413567809
Gid	39...7
DTB	0x0000000000000000
Start Time	2014-05-16 16:47:22 UTC+0000

The process' name is odd, possibly bordering on the suspicious. Its UID also indicates that this process is very likely not a legitimate process. Under Linux, as with many UNIX systems, UIDs are a 32-bit number; thus, the maximum UID a modern Linux system can have is 4,294,967,296. However, numbers this high are, at the very least, irregular. Moreover, so too is its GID.

Currently, there is no indication that this process is malicious as it could in fact be a remnant in memory left over from a previous process (or thread) or even from a previous operating system reboot. Nevertheless, this process's offset will be revisited later in this document.

It is worth attempting to dump this process from the memory image using the *linux_dump_map* plugin. This was performed using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_dump_map -p 2800 --dump-dir=.
```

This command resulted in no usable output or dumpfile. Other plugins that were tried included *linux_elfs*, *linux_procdump* and *linux_memmap*. None of them succeeded in dumping anything from memory or in providing more information.

3.3.6 Plugin linux_psxview

This plugin is related to the *psxview* plugin used for Windows memory investigations. However, this Linux-specific plugin makes use of very different data structures found only in Linux-based memory images.

Memory offsets are specified in terms of virtual addresses and the plugin uses five distinct algorithms for memory analysis. The first of these is *pslist*, which uses the same technique used by the *pslist* plugin (see Section 3.3.2). The second is *pid-hash*, which helps identify hidden processes (see Section 3.3.5). The third is *kmem_cache*, which examines the kernel's memory cache (see Section 3.3.3). Specifically, this cache stores information not only about ongoing processes but also metadata concerning terminated processes, sometimes even those which may have completed long ago, depending on the degree of process creation within the operating system. Finally, the field *Parents* "is populated by following the parent pointers of processes and threads found in the PID hash table" while the *Leaders* field "is populated by gathering the thread group leader pointer of each process and thread". [10, 12]

When working with this plugin it is important to identify those processes or threads that are obvious outliers. It is normal that the various field values vary a lot, but those that are too different from their surrounding may warrant additional inspection.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_psxview
```

The resulting output is too long to include here but can be found in Annex B.6. Nearly double the numbers of processes (279) were found using this plugin. They are the very same processes identified by plugin *linux_pidhashtable* (see Section 3.3.5) with the exception of three additional processes. These additional processes were:

- ---------- (this process had no valid name, PID or virtual address offset)
- swapper (PID 0)
- third instance of zeitgeist-datah

PID 2800 (process name: *?GQ ???*) was also identified by the *linux_psxview* plugin. Moreover, nothing specifically suspicious concerning the *zeitgeist-datah* processes could be identified, other than the fact that they have different entries in the table of Annex B.6 .

Finally, the *swapper* process is entirely legitimate for Linux and UNIX-like systems where PID 0 is typically reserved for kernel process *swapper* or *sched* (system scheduler) [11].

3.3.7 Summary

Performing Volatility process listings and analysis has shown that thus far, the only issue of note is a suspicious process found with name *?GQ ???* (with an unidentified PID), using both the *linux_psxview* and *linux_pidhashtable* plugins. Since attempts to dump this "process" have failed, and given the information obtained about it using the aforementioned plugins, it is very likely that it is in fact not a process but junk residing in memory. This would seem to be the logical conclusion to draw based on the available facts. However, further analyses of the memory image are still required.

Although nothing significant has been thus far established, the use of process listing and process scanning plugins is an important step in any memory investigation that should not be skipped as malware may leave behind indications of its presence. Each of the plugins presented in this step has the ability to provide clues or contextual information concerning the relationship between the various detailed processes and threads.

3.4 Step 4: Volatility history listing and system shells

In this step, various command shell listing plugins will be used to attempt to identify pertinent shell histories.

3.4.1 Plugin linux_bash

This particular plugin searches a memory image for command shell histories, similar to Volatility's Windows-based command history plugins. This is a brute force plugin in that it scans the entire memory image for signs of shell histories and as such may output erroneous information [10, 12].

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_bash -A
```

Running with the *-A* option can help ensure that all processes are scanned for shell history information, but it can take many hours to process a large memory image. It is also possible that the plugin will crash when used with this option. However, the option is useful because attackers may have copied the shell program (i.e. *bash*) to another name (i.e. */tmp/hsab*) and ran it to circumvent the manual detection of shell histories in memory. Tests have found that the same amount of information was identified when the plugin was used without the option. Of course, mileage will vary.

In a typical investigation, there could be hundreds or even thousands of lines of shell history to go over. Typically, after a system reboot, pre-existing shell histories will no longer be recoverable from memory; this, of course, is only a rule of thumb and there are times when pre-reboot data will remain intact in memory for recovery.

Relevant output generated by the plugin is listed in Table 6.

***Table 6**: Pertinent plugin output for linux_bash (pruned and sorted chronologically).*

PID	Name	Command Time	Command
1692	bash	2014-05-16 16:51:07 UTC+0000	mkdir /media/malware ; mount -t vboxsf Rootkits /media/malware
1692	bash	2014-05-16 16:51:49 UTC+0000	cd /media/malware/
1692	bash	2014-05-16 16:52:01 UTC+0000	mount -t vboxsf Rootkits /media/malware
1692	bash	2014-05-16 16:52:05 UTC+0000	cd /media/malware/
1692	bash	2014-05-16 16:52:17 UTC+0000	cd IVYL/
1692	bash	2014-05-16 16:52:19 UTC+0000	cd rootkit-master/
1692	bash	2014-05-16 16:53:10 UTC+0000	insmod *.ko
1692	bash	2014-05-16 16:53:20 UTC+0000	cat /proc/rtkit

While the above shell history information does show that data, possibly a rootkit source code was copied over from the host system to the guest VM system, a driver was also likely loaded into memory. This driver, as far as it is known, is the rootkit in question and the final command in the table attempts to query a new kernel structure for more information (see Section 1.6).

However, an attacker's shell command histories will not be retrievable in every case. Moreover, in a real-world scenario, one would not expect to find remnants of a shared VM folder in memory or the files/directories contained therein.

3.4.2 Plugin linux_bash_env

This new plugin has the ability to find various environment variables used by a command line shell. As such, this plugin has the potential to provide important clues concerning an attacker's actions against a suspect system.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_bash_env
```

Environment variables were only identified for PID 1556. What was identified for PID 1692 in the table below is a command, not an environment variable. Careful analysis of this plugin's output has revealed that nothing of use or importance could be found within the output listed in Table 7. In fact, the *dd* command listed as a *bash* shell environment variable is a left over remnant from a previous session of this VM.

***Table 7**: Plugin output for linux_bash_env.*

PID	Name	Variables
1556	bash	ORBIT_SOCKETDIR=/tmp/orbit-richard SSH_AGENT_PID=1319 TERM=xterm SHELL=/bin/bash XDG_SESSION_COOKIE=777b901babad8d3f6a4b67c100000005-1400258888.726668-1941620134 WINDOWID=62914598 GNOME_KEYRING_CONTROL=/tmp/keyring-nLdrWW GTK_MODULES=canberra-gtk-module USER=richard LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arj=01;31:*.taz=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lz=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.rar=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.axv=01;35:*.anx=01;35:*.ogv=01;35:

PID	Name	Variables
		.ogx=01;35:.aac=00;36:*.au=00;36:*.flac=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.axa=00;36:*.oga=00;36:*.spx=00;36:*.xspf=00;36: SSH_AUTH_SOCK=/tmp/keyring-nLdrWW/ssh SESSION_MANAGER=local/ubuntu-64:@/tmp/.ICE-unix/1252,unix/ubuntu-64:/tmp/.ICE-unix/1252 USERNAME=richard DEFAULTS_PATH=/usr/share/gconf/gnome.default.path XDG_CONFIG_DIRS=/etc/xdg/xdg-gnome:/etc/xdg PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games DESKTOP_SESSION=gnome PWD=/home/richard GDM_KEYBOARD_LAYOUT=us GNOME_KEYRING_PID=1233 LANG=en_US.UTF-8 GDM_LANG=en_US.utf8 MANDATORY_PATH=/usr/share/gconf/gnome.mandatory.path UBUNTU_MENUPROXY=libappmenu.so COMPIZ_CONFIG_PROFILE=ubuntu GDMSESSION=gnome SHLVL=1 HOME=/home/richard LANGUAGE=en_US:en GNOME_DESKTOP_SESSION_ID=this-is-deprecated LOGNAME=richard XDG_DATA_DIRS=/usr/share/gnome:/usr/local/share/:/usr/share/ DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-1c5rG8LUrV,guid=86fedc11154cd310d59c936b0000002e LESSOPEN=| /usr/bin/lesspipe %s WINDOWPATH=7 DISPLAY=:0 LESSCLOSE=/usr/bin/lesspipe %s %s COLORTERM=gnome-terminal XAUTHORITY=/var/run/gdm/auth-for-richard-TyTFyT/database _=/bin/su
1692	bash	dd if=/dev/fmem of=fmem.dd bs=1K count=800000

3.4.3 Plugin linux_psenv

This plugin is used to identify which environment variables and system shell were inherited or attributed to the various processes at their moment of instantiation.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_psenv | tr "\" "\n" | grep SHELL
```

The output from this plugin is not shown, as it contained no relevant information. Furthermore, all of the shell variables found within the output all used *bash* as their system shell, as per the various processes' environment variable settings (i.e. SHELL=/bin/bash).

3.4.4 Plugin linux_bash_hash

This new and unique plugin recovers the *bash* hash table kept in memory by the *bash* command line shell. *Bash* uses a hash table to keep track of commands and the number of times they were run. This plugin also provides the *-A* command line parameter which is used to scan the entire memory image for additional hash tables. Again, in so doing, if the memory image is too large the plugin could crash or take a very long time to run.

The plugin was run using the following command:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_bash_hash
```

The plugin was originally run with the *-A* but it crashed instead of producing useable results. Thus, the command was rerun without *-A* which produced the results shown in Table 8.

***Table 8**: Plugin output for linux_bash_hash.*

Pid	Name	Hits	Command	Full Path
1692	bash	2	umount	/bin/umount
1692	bash	3	df	/bin/df
1692	bash	4	cat	/bin/cat
1692	bash	4	mount	/bin/mount
1692	bash	1	insmod	/sbin/insmod
1692	bash	3	mkdir	/bin/mkdir
1692	bash	12	ls	/bin/ls
1692	bash	1	mesg	/usr/bin/mesg

Upon a thorough examination of the above listed output, the only truly interesting command is *insmod*, which was *su'ed* into by the logged in user. We know this command is running under *su* as based on the output from the *linux_psaux* plugin.

This command is used to load kernel modules (or drivers) into kernel-space. Thus, something was likely loaded, unless said loading failed, for which information is not currently available.

3.4.5 Summary

Performing Volatility history listing and system shells has demonstrated that searching for shell command histories can produce rewards, especially if a system's memory is acquired within a few hours of compromise (or possibly more if the system is quiescent).

However, both what is recovered and its pertinence can vary greatly between investigations and, as such, investigators and incident handlers must remember that these *bash*-based plugins

represent only one small piece of the analysis. These plugins rely on the *bash* shell, which is not always the system or user default shell; thus, these plugins do have their limits.

In using these four plugins, only the *linux_bash* and *linux_bash_hash* plugins found evidence of commands used for the loading of a potential rootkit. At least, these commands are suspicious in a day-to-day environment— normal users should not use them.

3.5 Step 5: Volatility file detection and dumping

In this step, various plugins will be used to attempt to isolate and dump important or suspicious files for further analysis.

3.5.1 Plugin linux_lsof

This plugin lists all open files, sockets, pipes, directories and other objects that the system currently has open for a given process, a list of processes, or all processes. This plugin functions similarly to the UNIX/Linux command *lsof*; however, it does not in any way list the same number of files or details as the real *lsof* command does. For example, a typical Linux system running with X Windows will have at least several thousand more open filesystem objects[6]. However, in using this plugin, it is likely that less than half of these will actually be open.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_lsof
```

Correlating the output from this plugin against those from the *linux_psaux* and *linux_psxview* plugins resulted in no actionable information or additional clues about the underlying infection. Moreover, this plugin does not have the ability to provide information concerning hidden processes and rootkits. The plugin succeeded in identifying 1,336 objects. After going over this output, nothing suspicious could be found therein (e.g. */proc/rtkit*).

3.5.2 Plugin linux_dentry_cache

This plugin recovers, files from the active mount point of each filesystem in memory, assuming they are still resident in memory or have not been paged out. Apparently, the plugin also has the ability to recover deleted files from copies in memory, assuming the aforementioned caveats [10, 12].

The reason this plugin does not work is that it supports SLAB-only based kernels, not SLUB-based kernels [4, 5, 6].

[6] This test was carried out on the infected VM after memory acquisition using the command “lsof | wc -l”.

3.5.3 Plugin linux_enumerate_files

This plugin is used to list the various files referenced by the filesystem cache, both those from the actual disk filesystem(s) and the kernel's pseudo-files. However, the vast majority of the disk-based files referenced therein will not actually reside within the cache itself unless the cache is extraordinarily large and fresh, perhaps being found only on very large memory systems (64+ GiB RAM).

Nevertheless, this plugin often times has the ability to enumerate far more files than the *linux_lsof* plugin; as such, it should be used when the latter fails to find anything of interest.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_enumerate_files
```

The plugin did not succeed in locating */proc/rtkit* or evidence of the rootkit within the disk-based portion of the filesystem cache. However, it did find evidence of the rootkit's source code files, compiled kernel module and ZIP archive from the VirtualBox host-shared folder. However, the reader should not take these into consideration as the virtual machine's memory was imaged immediately after infection, something which will almost never happen in the real-world, where infections are only found hours, days and sometimes weeks (or even months) after the fact. Also, these were found on a VM shared folder, not something likely to be found in a real-world situation.

3.5.4 Plugin linux_kernel_opened_files

This new plugin is used to list files and other filesystem objects that are opened or used from within the kernel itself, somewhat similar to plugin *linux_lsof*.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_kernel_opened_files
```

The plugin appears to have worked as it emitted no errors, but it generated no output. Thus, it can only be concluded that it either did not work and generated no errors or worked but found nothing (or there was nothing to report). This is in contrast to report [9] where the plugin failed and emitted an error likely caused by a missing Python library or Volatility dependency.

3.5.5 Plugin linux_proc_maps

This very powerful plugin can be used to learn important information about the underlying system as a whole or about one or more specific processes. Specifically, this plugin is used to identify process metadata including the name and location of running processes, shared libraries, stacks, inodes and memory address ranges.

The plugin was run using the following commands:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_proc_maps | tail -n +3 > proc_maps.txt

$ cat proc_maps.txt | awk '{print $9}' | sort | uniq > proc_maps_2.txt
```

The first command uses *tail* to remove the first two lines of output that is appended by Volatility, which is then redirected to file *proc_maps.txt*. The second command reduces the plugin's 15,162 lines of output to a manageable 566. The *sort* utility sorts all output generated by the second command alphanumerically while the *uniq* utility removes all duplicate lines of output. Although the new output is far shorter than the original output, it is still too lengthy to include herein.

After analysing the shorter output, nothing out of the ordinary was found.

3.5.6 Plugin linux_proc_maps_rb

This plugin is the same as the *linux_proc_maps* plugin except that it relies on the kernel's red-black process mapping structure. Exactly what that is or how it works is outside the scope of this work as it deep-dives into kernel structures. It is another technique for attempting to identify process metadata including the name and location of running processes, shared libraries, stacks, inodes and memory address ranges.

The plugin was run using the following commands:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_proc_maps_rb | tail -n +3 >
proc_maps_rb.txt

$ cat proc_maps_rb.txt | awk '{print $9}' | sort | uniq > proc_maps_rb2.txt
```

The plugin has reproduced the same exact output as generated by the *linux_proc_maps* plugin, thus no further analysis will be detailed herein.

3.5.7 Plugin linux_find_file

3.5.7.1 Running the plugin

This particular plugin can be used to not only dump pre-identified files from the memory image (using information obtained from other plugins) but it can also list all filesystem objects with an open handle in memory. It will often list far more objects than *linux_proc_maps* or *linux_lsof*. However, it works differently than *linux_proc_maps* and *linux_lsof* do . Thus, when seeking out abnormal libraries and process names, plugin *linux_lsof* should be used first, followed by *linux_proc_maps* then *linux_find_file*.

The output of the *linux_find_file* plugin lists not only the inode number and memory reference but also provides the full name of the filesystem object with the open handle. This plugin provides

useful information that can be used to readily dump one or more objects from the memory image, but only if they are cached in memory.

However, this plugin is not designed for at large data recovery of cached filesystem objects held within the memory image. For that, the *linux_recover_filesystem* plugin should be used. Also, not every file with a handle in memory can be recovered from the memory image, as that file may not currently reside within the filesystem cache.

The plugin was run using the following command:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_find_file -L > find_files.txt
```

Text file *find_files.txt* contained a listing of 14,495 unique filesystem objects. Unless actionable intelligence was made available from one of the previous plugins (which it was not), this list of objects will have to be examined manually to search for anomalies. Such a task may take several hours to thoroughly inspect. Looking for anomalies when one does not know Linux very well is very difficult, and sometimes just not possible.

While examining the plugin's output, various files including multiple open source rootkit packages, were found atop */media/malware*, the mounted VirtualBox shared connection used to transfer the rootkit's source code to the underlying virtual machine. What the reader should be concentrating on while examining this plugin's output are the files that are directly related to this investigation because these types of shares (containing malware) will most likely not be found in a real-world situation.

However, for the sake of understanding how this plugin functions with respect to 64-bit inodes (the previous Linux memory analysis reports examined 32-bit Linux systems), the information obtained from this plugin can be found in Table 9.

***Table 9**: Plugin output for linux_find_file*
(suspicious objects from the mounted virtual machine share; sorted by Inode Number).

Inode Number	Inode	File Path	Dumpable
18	0xffff8801151b1300	/media/malware/ubuntu/IVYL/rootkit-master.zip	No
20	0xffff880114485c80	/media/malware/ubuntu/IVYL/rootkit-master/rt.o	No
21	0xffff8801147bc4c0	/media/malware/ubuntu/IVYL/rootkit-master/.gitignore	No
22	0xffff880036a76720	/media/malware/ubuntu/IVYL/rootkit-master/Module.symvers	No
23	0xffff88010a284000	/media/malware/ubuntu/IVYL/rootkit-master/polis_paper.tex	No
24	0xffff8801151b1a20	/media/malware/ubuntu/IVYL/rootkit-master/rt.ko	No

Inode Number	Inode	File Path	Dumpable
25	0xffff880036998000	/media/malware/ubuntu/IVYL/rootkit-master/modules.order	No
26	0xffff880036998260	/media/malware/ubuntu/IVYL/rootkit-master/rt.mod.c	No
27	0xffff8800369984c0	/media/malware/ubuntu/IVYL/rootkit-master/.rt.mod.o.cmd	No
28	0xffff880036998720	/media/malware/ubuntu/IVYL/rootkit-master/README.md	No
29	0xffff880036998980	/media/malware/ubuntu/IVYL/rootkit-master/.rt.o.cmd	No
30	0xffff880036998be0	/media/malware/ubuntu/IVYL/rootkit-master/rt.mod.o	No
31	0xffff880036998e40	/media/malware/ubuntu/IVYL/rootkit-master/.rt.ko.cmd	No
32	0xffff8800369990a0	/media/malware/ubuntu/IVYL/rootkit-master/.tmp_versions	No

N.B.: The fourth column was added by the author and is not part of the plugin's output. The "Dumpable" column is based on the results obtained in Section 3.5.7.2.

These files have the distinct look of an installation package (with source code) for a Linux rootkit. However, none of them was recoverable, as was the case for report [9] where the various source code-compiled *.*so* files were completely recovered. Nevertheless, even had any been recoverable, they would not likely be found in a real-world investigation as having come from a VM shared folder.

Nevertheless, the commands used to attempt memory-based file recovery would be:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_find_file -i 0xffff8801151b1a20 -O rt.ko

…

$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_find_file -i 0xffff8801151b1300 -O rootkit-
master.zip
```

In all, it was attempted to recover 17 files in total, including source code and other data files. However, not a single one was recovered.

3.5.8 Plugin linux_recover_filesystem

This very powerful plugin can recreate the filesystem based on the contents of the memory image's filesystem cache. All modern Linux systems use such a cache although the amount of memory dedicated to such a cache can be configured.

Running this plugin can take many hours, depending on various factors, including the size of the memory image, the source and destination disks' speed, whether the source and destination disk are the same disk, etc. In this case, using the same disk for both source and destination, it took approximately 3 hours to recover the filesystem cache. This is the only Linux plugin examined herein which requires being run as root. Many of the files written back to disk have root-specific permissions that cannot be handled by a non-root user. Extended filesystem attributes are not preserved when the plugin is recovering the data from the filesystem cache.

The plugin was run using the following command:

```
$       mkdir recover_fs

$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_recover_filesystem -D recover_fs
```

The plugin succeeded in recovering 11,537 files and 2,885 directories for a total of approximately 5,170,423,398 (4.93 GiB) of consumed disk space within directory *recover_fs*. This was odd since the total allocated memory to the virtual machine was 4 GiB. Further investigation revealed that the mounted shared directory from the host system, */media/malware*, was consuming most of this space. Therein, a copy of the uninfected memory dumpfile *ubuntu_1104_base.mem* was found consuming 4,433,464,300 bytes (4.13 GiB). However, its SHA1 hash was not at all the same indicating that this file was no longer the same (see Section 1.7.1); further analysis revealed that this file was completely empty.

No evidence of the disk-based rootkit (e.g. */proc/rtkit*, */rootkit*), its source code, ZIP archive or compiled kernel module could be found within directory *recover_fs*.

3.5.9 Summary

Performing Volatility file detection and dumping has demonstrated that this rootkit, which has the ability to modify both *procfs* and *readdir* calls (see Section 1.4), apparently has the ability to hide itself from all file listing and related dumping plugins.

What was found concerning the rootkit infection was limited to the virtual machine share set up between the VM and host system to transfer the rootkit's ZIP archive to the VM for compilation and infection. While the files from this share were visible, they were not dumpable. Again, in a real-world situation, it is unlikely that an investigator or incident handler would be fortunate enough to find all this information still readily available in a system's captured memory.

Nevertheless, in going over the various possible file listing and related dumping plugins, it was possible to assess the various capabilities of Volatility, which in the opinion of the author, are quite remarkable.

Finally, one plugin which was not listed in this step but which was experimented with was the *linux_tmpfs* plugin, which was found to be non-functional atop both Fedora 17 and 21.

3.6 Step 6: Volatility kernel-specific analyses

In this step, various plugins will be used to attempt to identify the presence of a kernel-level rootkit using kernel-specific Volatility-based checks.

3.6.1 Plugin linux_lsmod

This plugin lists all visible Linux kernel modules running on the system, similar to the Linux *lsmod* command. Unlike *lsmod*, this plugin provides the base address for every detected kernel module.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_lsmod
```

This resulted in the modules listed in Annex B.7. The *-P* parameter can be used to list all specified module input parameters. The *-S* parameter can be used to list all memory areas used by a given kernel module. Looking at the output, nothing appears out of the ordinary. All the kernel modules listed appear legitimate.

3.6.2 Plugin linux_check_modules

This powerful plugin performs kernel module differencing, looking for inconsistencies between the different kernel module lists. It compares the information reported by kernel structure */proc/modules* against */sys/modules*. Through this plugin, it may be possible to corroborate the results of the *linux_hidden_modules* plugin (next section).

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_hidden_modules
```

This plugin took several minutes to complete but did not succeed in finding any pertinent information. Thus, it appears that this rootkit has the ability to hide from both */proc/modules* and */sys/modules*, something not commonly seen in Linux rootkits.

3.6.3 Plugin linux_hidden_modules

This plugin finds hidden kernel modules that have been unlinked from the list of modules. The plugin scans the entire memory image for LKM structures and then compares this information against the list of reported modules [10, 12]. This is a highly useful plugin as it can reveal information about hard to detect rootkits. Although the *linux_check_modules* plugin also has the ability to detect hidden kernel modules, they work through vastly different mechanisms.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_hidden_modules
```

This plugin succeeded in finding a hidden kernel module named *rt* at offset 0xffffffffa02bf020.

Interestingly, the suspicious module's name is the same as the loaded rootkit (*rt.ko*; see Section 1.6). The detected module should be dumpable using *linux_moddump*.

3.6.4 Plugin linux_moddump

The *linux_moddump* program is very similar to its Windows counterpart, *moddump*. Both versions of this plugin have the ability to dump all visible kernel modules (device drivers for Windows). Furthermore, both plugins have the ability to dump hidden modules (drivers) if a base address is specified. Thus, if there are indications of kernel-level malware activity and the module is not hidden, or at least a base address is known, the investigator/incident handler can dump it.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_moddump -b 0xffffffffa02bf020 -D .
```

The plugin created dumpfile *rt.0xffffffffa02bf020.lkm*, with a file size of 2,691,898 bytes (2.56 MiB) and a SHA1 hash of AE631B095A23F51450378211B8AA60237631CC6B. This file is much larger than the original compiled rootkit, *rt.ko*, found in Section 1.6.

A detailed *strings* analysis of the dumpfile reveals that this file is in fact the rootkit but that it also contains other memory residue, some of it very likely leftovers from other processes, threads, or modules. Although the rootkit module was successfully dumped, it is not as it should have been as it should have been equal in both size and hash value to the actual rootkit module, as the plugin is supposed to recreate the missing ELF header and properly aligns the pages. As such, further analyses will be conducted against this memory image to establish if additional indicators of compromise can be ascertained.

3.6.5 Plugin linux_check_fop

An interesting plugin, it is used to verify if there are hooks in the kernel with respect to opened files and validates that each file's *file_operation* structure is intact. When a potential hook is discovered, the plugin will generate output [10].

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_check_fop
```

Running this plugin produced 788 lines of output that can be found in Annex B.8. Looking at that output, it is evident that this rootkit has hooked many instances of *readdir()*.

3.6.6 Plugin linux_check_syscall

This plugin searches a memory image for hooked system calls (syscalls). If the plugin detects something, it will print HOOKED followed by the expected system call [10].

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_check_syscall
```

Running the plugin resulted in no hooked system calls. This could be because there are none or because the rootkit successfully hid them.

3.6.7 Plugin linux_check_afinfo

This plugin validates two network protocol-specific kernel structures, *file_operations* and *sequence_operations* against kernel structures *tcp6_seq_afinfo*, *tcp4_seq_afinfo*, *udp6_seq_afinfo*, *udp4_seq_afinfo*, *udplite6_seq_afinfo* and *udplite4_seq_afinfo*. Essentially, this plugin attempts to determine if any of these structures have been tampered with [10].

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_check_afinfo
```

The plugin did not provide any output thereby indicating that no abnormalities had been detected.

3.6.8 Summary

Performing Volatility kernel-specific analyses has demonstrated that some of the various kernel-specific plugins have positively identified that a rootkit is at work. Specifically, the *linux_hidden_modules* and *linux_check_fop* plugins have found clear evidence of rootkit infection while plugin *linux_moddump* was used to dump the rootkit module to disk.

Interestingly, the *linux_hidden_modules* and *linux_check_modules* were not able to corroborate one another, as they typically do. Thus, it must be concluded that this rootkit has the ability to modify the results from kernel pseudo-file */sys/modules*, which, when compared against */proc/modules,* should have yielded some indication of rootkit infection.

The other plugins, *linux_lsmod*, *linux_check_syscall* and *linux_check_afinfo*, did not find any additional indications of rootkit activity.

Finally, while the module dumped to disk was identified as the rootkit containing the same strings as the compiled rootkit, the memory-dumped version was much larger as we were expecting the plugin to correctly dump only the LKM.

3.7 Step 7: Volatility network-specific plugins

This step will examine the use of various network-based plugins as they pertain to this investigation.

3.7.1 Plugin linux_route_cache

This plugin produces information concerning the system's routing cache, which includes both ongoing and recently terminated communications. This plugin also lists additional information including the underlying system's IP address and various gateway addresses in use, which could be modified by certain malware to avoid detection.

The plugin was run using the following command:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_route_cache | sort | uniq
```

The information presented in Table 10 does not accurately reflect the various IP addresses attributed to the infected virtual machine. The actual IP address of the virtual machine is 10.0.2.15, which is incorrectly attributed to interface *lo*, but which should be allocated to interface *eth0*. The gateway address, 10.0.2.2, is correct as the virtual machine was configured to use NAT. However, the IP address of the host system, 192.168.0.102, is not found herein, which is normal, as this address does not have an actual impact on the virtual machine's network routing table. The host system's DSL router's address was 192.168.0.1, which was the gateway address for accessing the Internet. Finally, addresses 91.189.89.199 and 91.189.94.4, upon having looked them up, are both attributable to Canonical Ltd[7].

***Table 10**: Plugin output for linux_route_cache (sorted by interface).*

Interface	Destination	Gateway
eth0	91.189.89.199	10.0.2.2
eth0	91.189.94.4	10.0.2.2
eth0	192.168.0.1	10.0.2.2
lo	10.0.2.15	10.0.2.15
lo	127.0.0.1	127.0.0.1

Thus, appropriate context is required to make sense of this plugin's output.

3.7.2 Plugin linux_netstat

This plugin performs the equivalent of the UNIX/Linux *netstat* command in that it is used to print information concerning network connections (the actual *netstat* command does far more).

The plugin was run using the following command:

[7] Canonical is the maker of Ubuntu Linux.

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_route_cache linux_netstat -v | grep -P
'(TCP|UDP)'
```

The information revealed by the output shown in Table 11 indicates that there is nothing out of the ordinary going on with respect to network communications. Running the plugin without the *grep* statement also revealed nothing out of the ordinary.

***Table 11**: Plugin output for linux_netstat for TCP/UDP (sorted by Type and Socket/Inode).*

Type	Socket / Inode	Process	Associated disk-based file
UDP	0.0.0.0	: 5353 0.0.0.0	: 0 avahi-daemon/446
UDP	::	: 5353 ::	: 0 avahi-daemon/446
UDP	0.0.0.0	:36575 0.0.0.0	: 0 avahi-daemon/446
UDP	::	:41003 ::	: 0 avahi-daemon/446
UDP	0.0.0.0	: 68 0.0.0.0	: 0 dhclient/523
TCP	::1	: 631 ::	: 0 LISTEN cupsd/1017
TCP	127.0.0.1	: 631 0.0.0.0	: 0 LISTEN cupsd/1017

3.7.3 Plugin linux_list_raw

This new Volatility plugin is designed to list all processes running with raw (or promiscuous) sockets, which can be helpful in determining if a sniffer or other possibly malicious service (or daemon or malware) was active atop the suspect system.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_list_raw
```

While it is currently unknown if the system DHCP process (dhclient) shown in Table 12 should be running with a raw socket, it does not in itself appear to be malicious in nature.

***Table 12**: Plugin output for linux_list_raw.*

Process	PID	File Descriptor	Inode
dhclient	523	5	7867

3.7.4 Summary

Performing Volatility network-specific analyses has demonstrated that not all rootkits and malware take advantage of Internet facing connections. Plugin *linux_sk_buff_cache* was not used because there was no suspicious communications that were in process or that had recently ended.

There was no point in running plugin *linux_netfilter* as there was no firewall running, as per the kernel's list of loaded modules (see Section 3.6.1 for details). There was also little reason to have believed, at least in the author's opinion, that running the *linux_arp* plugin would have revealed any additional information of interest.

The plugins used in this step have not been able to identify any additional information pertinent to this investigation, at least with respect to the network.

3.8 Step 8: Additional checks

This step will run additional checks to search for injected code, credential escalation attacks and indications of keylogger activity in order to identify certain telltale signs of some rootkits.

3.8.1 Plugin linux_malfind

This new plugin, similar to the Windows version, searches memory images for indications of code injection.

The plugin was run using the following command:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_malfind
```

The plugin found no indication of injected code within this memory image.

3.8.2 Plugin linux_check_creds

This plugin is used to check for processes with raised privileges, typical of certain types of rootkits.

The plugin was run using the following command:

```
$       volatility --profile=Linuxubuntu_1104_profilex64 -f
        ubuntu_1104_IVYL.mem linux_check_creds
```

The plugin found no indication of process elevation. The results might have been different had the rootkit's "root" shell been invoked (see Section 1.7 for details).

3.8.3 Plugin linux_apihooks

This plugin is used to check for API hooking [10, 12], which is sometimes known as inline hooking. This hooking technique is used by various malware to infect a system.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_apihooks
```

This plugin was found to be non-functional, at least atop Fedora 17 and 21, having aborted due to an obscure Volatility error.

3.8.4 Plugin linux_check_idt

This plugin checks a memory image for signs of hooking in the system Interrupt Descriptor Table (IDT) [10, 12]. If any of the IDTs appear to have been hooked, the plugin will issue HOOKED in lieu of the expected symbol name.

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_check_idt
```

The information in Table 13 indicates that nothing out of the ordinary has occurred to the system IDTs.

***Table 13**: Plugin output for linux_check_idt (sorted by index).*

Index	Address	Symbol
0x0	0xffffffff8100cc20	divide_error
0x1	0xffffffff815c3360	debug
0x2	0xffffffff815c3770	nmi
0x3	0xffffffff815c33a0	int3
0x4	0xffffffff8100cc40	overflow
0x5	0xffffffff8100cc60	bounds
0x6	0xffffffff8100cc80	invalid_op
0x7	0xffffffff8100cca0	device_not_available
0x8	0xffffffff8100ccc0	double_fault
0x9	0xffffffff8100ccf0	coprocessor_segment_overrun
0xa	0xffffffff8100cd10	invalid_TSS
0xb	0xffffffff8100cd40	segment_not_present
0xc	0xffffffff815c33e0	stack_segment
0xd	0xffffffff815c3480	general_protection
0xe	0xffffffff815c34b0	page_fault
0xf	0xffffffff8100cd70	spurious_interrupt_bug
0x10	0xffffffff8100cd90	coprocessor_error

Index	Address	Symbol
0x11	0xffffffff8100cdb0	alignment_check
0x12	0xffffffff815c3510	machine_check
0x13	0xffffffff8100cde0	simd_coprocessor_error
0x80	0xffffffff81048aa0	ia32_system_call

3.8.5 Plugins for keylogger detection (linux_check_tty and linux_keyboard_notifiers)

Both plugins can be used to help identify kernel-level keyloggers as each plugin uses a different mechanism. It is hoped that one of them will determine if a keylogger is present in this memory image having been introduced by the rootkit.

The following commands were issued:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_check_tty

$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_keyboard_notifier
```

The information in Table 14 indicates that nothing out of the ordinary has occurred to the system IDTs while plugin *linux_keyboard_notifier* produced no output.

***Table 14**: Plugin output for linux_check_tty (sorted by tty).*

Name	Address	Symbol
tty1	0xffffffff81386160	n_tty_receive_buf
tty2	0xffffffff81386160	n_tty_receive_buf
tty3	0xffffffff81386160	n_tty_receive_buf
tty4	0xffffffff81386160	n_tty_receive_buf
tty5	0xffffffff81386160	n_tty_receive_buf
tty6	0xffffffff81386160	n_tty_receive_buf
tty7	0xffffffff81386160	n_tty_receive_buf

Whereas the former plugin scans drivers for *tty* hooking, the latter plugin scans for hooked kernel callbacks [10, 12].

3.8.6 Plugin linux_check_evt_arm

This plugin searches for syscall hooking as they relate to the system's Exception Vector Table (EVT), which is closely related to the IDTs (see Section 3.8.4).

The plugin was run using the following command:

```
$ volatility --profile=Linuxubuntu_1104_profilex64 -f
ubuntu_1104_IVYL.mem linux_check_idt
```

This resulted in no useful output, indicating that the plugin found no indication of EVT syscalls hooking.

3.8.7 Summary

Although it was desirable to run plugin *linux_process_hollow*, it required the PID of one or more processes to test against (or an ELF base address), and since there were no suspicious processes to test, this plugin was not used. PID 2800, identified in Section 3.3.5, is entirely indicative of a leftover remnant in memory.

The plugins used in this step found no indication of keylogger activity, nor did they find any evidence of system hooks via EVT or IDT.

Finally, no indication of rootkit activity could be found. However, to be fair, no augmented root shell was opened with extended privileges in the VM (see Section 1.7) nor is it certain if this rootkit has a keylogging capability.

4 Conclusion

IVYL, the third rootkit analysed in this suite of reports (or tutorials), while simple with respect to its capabilities as compared to KBeast, was more difficult to identify. This specific report looked at and used many of the various Volatility plugins, far more than in the first two reports. In the end, the plugin that definitively identified the rootkit was *linux_hidden_modules* but when the LKM was dumped using *linux_moddump*, the dumped LKM was several magnitudes larger than the actual rootkit. Thus, because of this, additional analyses were carried out in the hopes of better understanding the infection.

As mentioned in several locations throughout the report, even though the VM shared folder and its files/directories were visible (as they pertained to the rootkit), they were never dumpable or recoverable. Moreover, in a real-world situation, it would be very unlikely that an investigator/incident handler would see a shared folder with all this evidence readily available.

This report has shown investigators/incident handlers what to look for when the majority of useful (and non-reverse engineering) Volatility plugins have been exhausted and turned up empty—that is to say they show no specific evidence of malware infection.

Again, as with the two previous Linux memory analysis reports, this rootkit was not identified as infected, malicious or suspicious by VirusTotal which that day used 57 different scanners to scan the uploaded rootkit sample. This is somewhat shocking considering that the rootkit is nearly two years old and its source code is available to anyone for modification or direct use.

Finally, this case study will have hopefully demonstrated to investigators/incident handlers how to systematically proceed with investigating a suspected Linux-based memory image and determine if it has been infected or set up for use by a userland rootkit.

References

[1] Hiler, Arkadiusz (ivyl) and t3hknr. Sample Rootkit for Linux. Readme text file. GitHub. August 2012. https://github.com/ivyl/rootkit.

[2] Hiler, Arkadiusz (ivyl). Simple Linux Rookit. Informative web site. 2013. http://ivyl.0xcafe.eu/2012/10/27/simple-linux-rootkit/.

[3] YobiWiki. RAM analysis: Misc notes on physical RAM analysis. Online documentation. October 2013. http://wiki.yobi.be/wiki/RAM_analysis.

[4] Kim, Joonsoo. How does the SLUB allocator work. Presentation. LGE CTO SWP Lab. Unknown date. http://events.linuxfoundation.org/images/stories/pdf/klf2012_kim.pdf.

[5] Wikipedia. Slab allocation. Online encyclopaedic entry. Wikimedia Foundation Inc. July 2014. http://en.wikipedia.org/wiki/Slab_allocation.

[6] Wikipedia. SLUB (software). Online encyclopaedic entry. Wikimedia Foundation Inc. August 2014. http://en.wikipedia.org/wiki/SLUB_(software).

[7] Volatility team. LinuxMemoryForensics: Instructions on how to access and use the Linux support. Online documentation. September 2013. http://code.google.com/p/volatility/wiki/LinuxMemoryForensics.

[8] Carbone, Richard. Malware memory analysis of the KBeast rootkit: Investigating publicly available Linux rootkits using the Volatility memory analysis framework. Scientific Report (in preparation for publishing). Defence Research & Development Canada – Valcartier. September 2014.

[9] Carbone, Richard. Malware memory analysis of the Jynx2 Linux rootkit: Investigating publicly available Linux rootkits using the Volatility memory analysis framework. Scientific Report. DRDC-RDDC-2014-R176. Defence Research & Development Canada – Valcartier. October 2014.

[10] Volatility. LinuxCommandReference23: A command reference for Linux. Unknown date. http://code.google.com/p/volatility/wiki/LinuxCommandReference23.

[11] Wikipedia. Process identifier. Online encyclopaedic entry. Wikimedia Foundation Inc. April 2014. http://en.wikipedia.org/wiki/Process_identifier.

[12] Hale Ligh, Michael; Case, Andrew et al. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Max Memory. Book. John Wiley & Sons. July 2014.

[13] ForensicsWiki. Ssdeep. Online information. ForensicsWiki. October 2010.

This page intentionally left blank.

Annex A Volatility 2.4 Linux-based plugins

Table A.1 is a complete list of the default Linux-based plugins provided by Volatility's 2.4 stable release.

Table A.1: *List of Volatility 2.4 plugins.*

Plugin	**Capability (as per Volatility --info output)**
linux_apihooks	Checks for userland apihooks
linux_arp	Print the ARP table
linux_banner	Prints the Linux banner information
linux_bash	Recover bash history from bash process memory
linux_bash_env	Recover bash's environment variables
linux_bash_hash	Recover bash hash table from bash process memory
linux_check_afinfo	Verifies the operation function pointers of network protocols
linux_check_creds	Checks if any processes are sharing credential structures
linux_check_evt_arm	Checks the Exception Vector Table to look for syscall table hooking
linux_check_fop	Check file operation structures for rootkit modifications
linux_check_idt	Checks if the IDT has been altered
linux_check_inline_kernel	Check for inline kernel hooks
linux_check_modules	Compares module list to sysfs info, if available
linux_check_syscall	Checks if the system call table has been altered
linux_check_syscall_arm	Checks if the system call table has been altered
linux_check_tty	Checks tty devices for hooks
linux_cpuinfo	Prints info about each active processor
linux_dentry_cache	Gather files from the dentry cache
linux_dmesg	Gather dmesg buffer
linux_dump_map	Writes selected memory mappings to disk
linux_elfs	Find ELF binaries in process mappings
linux_enumerate_files	Lists files referenced by the filesystem cache
linux_find_file	Lists and recovers files from memory
linux_hidden_modules	Carves memory to find hidden kernel modules

Plugin	Capability (as per Volatility --info output)
linux_ifconfig	Gathers active interfaces
linux_info_regs	It's like 'info registers' in GDB. It prints out all the
linux_iomem	Provides output similar to /proc/iomem
linux_kernel_opened_files	Lists files that are opened from within the kernel
linux_keyboard_notifiers	Parses the keyboard notifier call chain
linux_ldrmodules	Compares the output of proc maps with the list of libraries from libdl
linux_library_list	Lists libraries loaded into a process
linux_librarydump	Dumps shared libraries in process memory to disk
linux_list_raw	List applications with promiscuous sockets
linux_lsmod	Gather loaded kernel modules
linux_lsof	Lists open files
linux_malfind	Looks for suspicious process mappings
linux_memmap	Dumps the memory map for linux tasks
linux_moddump	Extract loaded kernel modules
linux_mount	Gather mounted fs/devices
linux_mount_cache	Gather mounted fs/devices from kmem_cache
linux_netfilter	Lists Netfilter hooks
linux_netstat	Lists open sockets
linux_pidhashtable	Enumerates processes through the PID hash table
linux_pkt_queues	Writes per-process packet queues out to disk
linux_plthook	Scan ELF binaries' PLT for hooks to non-NEEDED images
linux_proc_maps	Gathers process maps for linux
linux_proc_maps_rb	Gathers process maps for linux through the mappings red-black tree
linux_procdump	Dumps a process's executable image to disk
linux_process_hollow	Checks for signs of process hollowing
linux_psaux	Gathers processes along with full command line and start time
linux_psenv	Gathers processes along with their environment
linux_pslist	Gather active tasks by walking the task_struct->task list
linux_pslist_cache	Gather tasks from the kmem_cache

Plugin	Capability (as per Volatility --info output)
linux_pstree	Shows the parent/child relationship between processes
linux_psxview	Find hidden processes with various process listings
linux_recover_filesystem	Recovers the entire cached file system from memory
linux_route_cache	Recovers the routing cache from memory
linux_sk_buff_cache	Recovers packets from the sk_buff kmem_cache
linux_slabinfo	Mimics /proc/slabinfo on a running machine
linux_strings	Match physical offsets to virtual addresses (may take a while, VERY verbose)
linux_threads	Prints threads of processes
linux_tmpfs	Recovers tmpfs filesystems from memory
linux_truecrypt_passphrase	Recovers cached Truecrypt passphrases
linux_vma_cache	Gather VMAs from the vm_area_struct cache
linux_volshell	Shell in the memory image
linux_yarascan	A shell in the Linux memory image

This page intentionally left blank.

Annex B Plugin output and listings

This annex provides the various outputs and listings for the different plugins used throughout this report that are too lengthy to fit within the main text.

B.1 Output for plugin linux_dmesg

The following output was generated by the Volatility *linux_dmesg* plugin (see Section 3.2.3):

```
[2314885531810281020.2314885531] ] Initializing cgroup subsys cpuset
<6>[    0.000000] Initializing cgroup subsys cpu
<5>[    0.000000] Linux version 2.6.38-8-generic (buildd@allspice) (gcc
version 4.5.2 (Ubuntu/Linaro 4.5.2-8ubuntu3) ) #42-Ubuntu SMP Mon Apr 11
03:31:24 UTC 2011 (Ubuntu 2.6.38-8.42-generic 2.6.38.2)
<6>[       0.000000] Command line: BOOT_IMAGE=/vmlinuz-2.6.38-8-generic
root=UUID=45fdcb1c-c3c7-4c98-9ac3-7f8acf84ac26    ro    quiet    splash
vt.handoff=7
<6>[    0.000000] BIOS-provided physical RAM map:
<6>[       0.000000]    BIOS-e820:  0000000000000000  -  000000000009fc00
(usable)
<6>[       0.000000]    BIOS-e820:  000000000009fc00  -  00000000000a0000
(reserved)
<6>[       0.000000]    BIOS-e820:  00000000000f0000  -  0000000000100000
(reserved)
<6>[       0.000000]    BIOS-e820:  0000000000100000  -  00000000dfff0000
(usable)
<6>[    0.000000]  BIOS-e820: 00000000dfff0000 - 00000000e0000000 (ACPI
data)
<6>[       0.000000]    BIOS-e820:  00000000fffc0000  -  0000000100000000
(reserved)
<6>[       0.000000]    BIOS-e820:  0000000100000000  -  0000000120000000
(usable)
<6>[    0.000000] NX (Execute Disable) protection: active
<6>[    0.000000] DMI 2.5 present.
<7>[       0.000000]  DMI:  innotek  GmbH  VirtualBox/VirtualBox,  BIOS
VirtualBox 12/01/2006
<7>[    0.000000] e820 update range: 0000000000000000 - 0000000000010000
(usable) ==> (reserved)
<7>[    0.000000] e820 remove range: 00000000000a0000 - 0000000000100000
(usable)
<6>[    0.000000] No AGP bridge found
<6>[    0.000000] last_pfn = 0x120000 max_arch_pfn = 0x400000000
<7>[    0.000000] MTRR default type: uncachable
<7>[    0.000000] MTRR variable ranges disabled:
<6>[      0.000000] x86 PAT enabled: cpu 0, old 0x7040600070406, new
0x7010600070106
<6>[    0.000000] CPU MTRRs all blank - virtualized system.
<6>[    0.000000] last_pfn = 0xdfff0 max_arch_pfn = 0x400000000
<6>[    0.000000] found SMP MP-table at [ffff88000009fff0] 9fff0
<7>[    0.000000] initial memory mapped : 0 - 20000000
<6>[    0.000000] init_memory_mapping: 0000000000000000-00000000dfff0000
<7>[    0.000000]  0000000000 - 00dfe00000 page 2M
<7>[    0.000000]  00dfe00000 - 00dfff0000 page 4k
<7>[    0.000000] kernel direct mapping tables up to dfff0000 @ 1fffa000-
20000000
<6>[    0.000000] init_memory_mapping: 0000000100000000-0000000120000000
<7>[    0.000000]  0100000000 - 0120000000 page 2M
<7>[       0.000000] kernel direct mapping tables up to 120000000 @
dffea000-dfff0000
<6>[    0.000000] RAMDISK: 366da000 - 37365000
<4>[    0.000000] ACPI: RSDP 00000000000e0000 00024 (v02 VBOX  )
```

```
<4>[    0.000000] ACPI: XSDT 00000000dfff0030 0003C (v01 VBOX   VBOXXSDT
00000001 ASL  00000061)
<4>[    0.000000] ACPI: FACP 00000000dfff00f0 000F4 (v04 VBOX   VBOXFACP
00000001 ASL  00000061)
<4>[    0.000000] ACPI: DSDT 00000000dfff0470 01B96 (v01 VBOX   VBOXBIOS
00000002 INTL 20100528)
<4>[    0.000000] ACPI: FACS 00000000dfff0200 00040
<4>[    0.000000] ACPI: APIC 00000000dfff0240 0005C (v02 VBOX   VBOXAPIC
00000001 ASL  00000061)
<4>[    0.000000] ACPI: SSDT 00000000dfff02a0 001CC (v01 VBOX   VBOXCPUT
00000002 INTL 20100528)
<7>[    0.000000] ACPI: Local APIC address 0xfee00000
<6>[    0.000000] No NUMA configuration found
<6>[    0.000000] Faking a node at 0000000000000000-0000000120000000
<6>[    0.000000] Initmem setup node 0 0000000000000000-0000000120000000
<6>[    0.000000]   NODE_DATA [000000011fffb000 - 000000011fffffff]
<7>[          0.000000]     [ffffea0000000000-ffffea0003ffffff]   PMD   ->
[ffff88011be00000-ffff88011f7fffff] on node 0
<4>[    0.000000] Zone PFN ranges:
<4>[    0.000000]   DMA      0x00000010 -> 0x00001000
<4>[    0.000000]   DMA32    0x00001000 -> 0x00100000
<4>[    0.000000]   Normal   0x00100000 -> 0x00120000
<4>[    0.000000] Movable zone start PFN for each node
<4>[    0.000000] early_node_map[3] active PFN ranges
<4>[    0.000000]     0: 0x00000010 -> 0x0000009f
<4>[    0.000000]     0: 0x00000100 -> 0x000dfff0
<4>[    0.000000]     0: 0x00100000 -> 0x00120000
<7>[    0.000000] On node 0 totalpages: 1048447
<7>[    0.000000]   DMA zone: 56 pages used for memmap
<7>[    0.000000]   DMA zone: 6 pages reserved
<7>[    0.000000]   DMA zone: 3921 pages, LIFO batch:0
<7>[    0.000000]   DMA32 zone: 14280 pages used for memmap
<7>[    0.000000]   DMA32 zone: 899112 pages, LIFO batch:31
<7>[    0.000000]   Normal zone: 1792 pages used for memmap
<7>[    0.000000]   Normal zone: 129280 pages, LIFO batch:31
<6>[    0.000000] ACPI: PM-Timer IO Port: 0x4008
<7>[    0.000000] ACPI: Local APIC address 0xfee00000
<6>[    0.000000] ACPI: LAPIC (acpi_id[0x00] lapic_id[0x00] enabled)
<6>[    0.000000] ACPI: LAPIC (acpi_id[0x01] lapic_id[0x01] enabled)
<6>[    0.000000] ACPI: IOAPIC (id[0x02] address[0xfec00000] gsi_base[0])
<6>[    0.000000] IOAPIC[0]: apic_id 2, version 17, address 0xfec00000,
GSI 0-23
<6>[    0.000000] ACPI: INT_SRC_OVR (bus 0 bus_irq 0 global_irq 2 dfl
dfl)
<6>[    0.000000] ACPI: INT_SRC_OVR (bus 0 bus_irq 9 global_irq 9 high
level)
<7>[    0.000000] ACPI: IRQ0 used by override.
<7>[    0.000000] ACPI: IRQ2 used by override.
<7>[    0.000000] ACPI: IRQ9 used by override.
<6>[    0.000000] Using ACPI (MADT) for SMP configuration information
<6>[    0.000000] SMP: Allowing 2 CPUs, 0 hotplug CPUs
<7>[    0.000000] nr_irqs_gsi: 40
<6>[       0.000000]  PM:  Registered  nosave  memory:  000000000009f000  -
00000000000a0000
<6>[       0.000000]  PM:  Registered  nosave  memory:  00000000000a0000  -
00000000000f0000
<6>[       0.000000]  PM:  Registered  nosave  memory:  00000000000f0000  -
0000000000100000
<6>[       0.000000]  PM:  Registered  nosave  memory:  00000000dfff0000  -
00000000e0000000
<6>[       0.000000]  PM:  Registered  nosave  memory:  00000000e0000000  -
00000000fffc0000
<6>[       0.000000]  PM:  Registered  nosave  memory:  00000000fffc0000  -
0000000100000000
<6>[    0.000000] Allocating PCI resources starting at e0000000 (gap:
e0000000:1ffc0000)
<6>[    0.000000] Booting paravirtualized kernel on bare hardware
```

```
<6>[          0.000000]  setup_percpu:  NR_CPUS:256  nr_cpumask_bits:256
nr_cpu_ids:2 nr_node_ids:1
<6>[    0.000000] PERCPU: Embedded 28 pages/cpu @ffff8800dfc00000 s84416
r8192 d22080 u1048576
<7>[          0.000000]  pcpu-alloc:  s84416  r8192  d22080  u1048576
alloc=1*2097152
<7>[    0.000000] pcpu-alloc: [0] 0 1
<4>[    0.000000] Built 1 zonelists in Node order, mobility grouping on.
Total pages: 1032313
<4>[    0.000000] Policy zone: Normal
<5>[       0.000000]  Kernel  command  line:  BOOT_IMAGE=/vmlinuz-2.6.38-8-
generic  root=UUID=45fdcb1c-c3c7-4c98-9ac3-7f8acf84ac26  ro  quiet  splash
vt.handoff=7
<6>[    0.000000] PID hash table entries: 4096 (order: 3, 32768 bytes)
<6>[    0.000000] Checking aperture...
<6>[    0.000000] No AGP bridge found
<7>[    0.000000] Calgary: detecting Calgary via BIOS EBDA area
<7>[     0.000000] Calgary: Unable to locate Rio Grande table in EBDA -
bailing!
<6>[    0.000000] Memory: 4041840k/4718592k available (5940k kernel code,
524804k absent, 151948k reserved, 5017k data, 956k init)
<6>[    0.000000] SLUB: Genslabs=15, HWalign=64, Order=0-3, MinObjects=0,
CPUs=2, Nodes=1
<6>[    0.000000] Hierarchical RCU implementation.
<6>[    0.000000]   RCU   dyntick-idle   grace-period   acceleration   is
enabled.
<6>[    0.000000]   RCU-based detection of stalled CPUs is disabled.
<6>[    0.000000] NR_IRQS:16640 nr_irqs:512 16
<6>[    0.000000] vt handoff: transparent VT on vt#7
<4>[    0.000000] Console: colour dummy device 80x25
<6>[    0.000000] console [tty0] enabled
<6>[    0.000000] allocated 41943040 bytes of page_cgroup
<6>[     0.000000] please try 'cgroup_disable=memory' option if you don't
want memory cgroups
<4>[    0.000000] Fast TSC calibration failed
<4>[    0.000000] TSC: Unable to calibrate against PIT
<6>[    0.000000] TSC: using PMTIMER reference calibration
<4>[    0.000000] Detected 3481.792 MHz processor.
<6>[      0.030004] Calibrating delay loop (skipped), value calculated
using timer frequency.. 6963.58 BogoMIPS (lpj=34817920)
<6>[    0.030008] pid_max: default: 32768 minimum: 301
<6>[    0.030027] Security Framework initialized
<6>[    0.030042] AppArmor: AppArmor initialized
<6>[    0.030044] Yama: becoming mindful.
<6>[      0.034296] Dentry cache hash table entries: 524288 (order: 10,
4194304 bytes)
<6>[      0.035384] Inode-cache hash table entries: 262144 (order: 9,
2097152 bytes)
<4>[    0.035578] Mount-cache hash table entries: 256
<6>[    0.040088] Initializing cgroup subsys ns
<4>[          0.040091]  ns_cgroup  deprecated:  consider  using  the
'clone_children' flag without the ns_cgroup.
<6>[    0.040094] Initializing cgroup subsys cpuacct
<6>[    0.040097] Initializing cgroup subsys memory
<6>[    0.040102] Initializing cgroup subsys devices
<6>[    0.040105] Initializing cgroup subsys freezer
<6>[    0.040107] Initializing cgroup subsys net_cls
<6>[    0.040109] Initializing cgroup subsys blkio
<6>[    0.040183] CPU: Physical Processor ID: 0
<6>[    0.040186] CPU: Processor Core ID: 0
<6>[    0.040189] mce: CPU supports 0 MCE banks
<6>[    0.046882] ACPI: Core revision 20110112
<6>[    0.047519] ftrace: allocating 24314 entries in 96 pages
<6>[    0.050121] Setting APIC routing to flat
<6>[    0.060277] ..TIMER: vector=0x30 apic1=0 pin1=2 apic2=-1 pin2=-1
<6>[     0.187051] CPU0: Intel(R) Core(TM) i7 CPU        X 000  @ 3.33GHz
stepping 02
```

```
<4>[     0.190000] APIC calibration not consistent with PM-Timer: 96ms
instead of 100ms
<6>[    0.190000] APIC delta adjusted to PM-Timer: 6250051 (6023013)
<6>[    0.190000] Performance Events: unsupported p6 CPU model 44 no PMU
driver, software events only.
<6>[    0.190000] Booting Node   0, Processors  #1 Ok.
<6>[    0.040000] mce: CPU supports 0 MCE banks
<4>[    0.350000] TSC synchronization [CPU#0 -> CPU#1]:
<4>[     0.350000] Measured 123400 cycles TSC warp between CPUs, turning
off TSC clock.
<6>[       0.350000] Marking TSC unstable due to check_tsc_sync_source
failed
<6>[    0.350041] Brought up 2 CPUs
<6>[    0.350043] Total of 2 processors activated (13888.93 BogoMIPS).
<6>[    0.350333] devtmpfs: initialized
<6>[    0.350505] print_constraints: dummy:
<4>[    0.350529] Time: 16:47:17  Date: 05/16/14
<6>[    0.350547] NET: Registered protocol family 16
<6>[    0.350697] ACPI: bus type pci registered
<6>[    0.350755] PCI: Using configuration type 1 for base access
<6>[    0.350676] Trying to unpack rootfs image as initramfs...
<4>[    0.360214] bio: create slab <bio-0> at 0
<7>[    0.360596] ACPI: EC: Look up EC in DSDT
<4>[     0.360895] ACPI: Executed 1 blocks of module-level executable AML
code
<6>[    0.360895] ACPI: Interpreter enabled
<6>[    0.360895] ACPI: (supports S0 S5)
<6>[    0.360895] ACPI: Using IOAPIC for interrupt routing
<6>[    0.362170] ACPI: No dock devices found.
<6>[    0.362174] HEST: Table not found.
<6>[       0.362178] PCI: Ignoring host bridge windows from ACPI; if
necessary, use "pci=use_crs" and report a bug
<6>[    0.362229] ACPI: PCI Root Bridge [PCI0] (domain 0000 [bus 00-ff])
<7>[     0.362342] pci_root PNP0A03:00: host bridge window [io  0x0000-
0x0cf7] (ignored)
<7>[     0.362346] pci_root PNP0A03:00: host bridge window [io  0x0d00-
0xffff] (ignored)
<7>[        0.362350] pci_root PNP0A03:00: host bridge window [mem
0x000a0000-0x000bffff] (ignored)
<7>[        0.362354] pci_root PNP0A03:00: host bridge window [mem
0xe0000000-0xffdfffff] (ignored)
<7>[    0.362394] pci 0000:00:00.0: [8086:1237] type 0 class 0x000600
<7>[    0.366407] pci 0000:00:01.0: [8086:7000] type 0 class 0x000601
<7>[    0.366746] pci 0000:00:01.1: [8086:7111] type 0 class 0x000101
<7>[    0.367008] pci 0000:00:01.1: reg 20: [io  0xd000-0xd00f]
<7>[    0.367189] pci 0000:00:02.0: [80ee:beef] type 0 class 0x000300
<7>[     0.370279] pci 0000:00:02.0: reg 10: [mem 0xe0000000-0xe7ffffff
pref]
<7>[    0.414473] pci 0000:00:03.0: [8086:100e] type 0 class 0x000200
<7>[    0.416203] pci 0000:00:03.0: reg 10: [mem 0xf0000000-0xf001ffff]
<7>[    0.423979] pci 0000:00:03.0: reg 18: [io  0xd010-0xd017]
<7>[    0.432796] pci 0000:00:04.0: [80ee:cafe] type 0 class 0x000880
<7>[    0.434649] pci 0000:00:04.0: reg 10: [io  0xd020-0xd03f]
<7>[    0.436379] pci 0000:00:04.0: reg 14: [mem 0xf0400000-0xf07fffff]
<7>[     0.441137] pci 0000:00:04.0: reg 18: [mem 0xf0800000-0xf0803fff
pref]
<7>[    0.452879] pci 0000:00:05.0: [8086:2415] type 0 class 0x000401
<7>[    0.453031] pci 0000:00:05.0: reg 10: [io  0xd100-0xd1ff]
<7>[    0.453141] pci 0000:00:05.0: reg 14: [io  0xd200-0xd23f]
<7>[    0.453809] pci 0000:00:06.0: [106b:003f] type 0 class 0x000c03
[4192904279556632624.4192904279] 0ee:cafe] type 0 class 0x000880
<7>[    0.434649] pci 0000:00:04.0: reg 10: [io  0xd020-0xd03f]
<7>[    0.436379] pci 0000:00:04.0: reg 14: [mem 0xf0400000-0xf07fffff]
<7>[     0.441137] pci 0000:00:04.0: reg 18: [mem 0xf0800000-0xf0803fff
pref]
<7>[    0.452879] pci 0000:00:05.0: [8086:2415] type 0 class 0x000401
<7>[    0.453031] pci 0000:00:05.0: reg 10: [io  0xd100-0xd1ff]
<7>[    0.453141] pci 0000:00:05.0: reg 14: [io  0xd200-0xd23f]
```

```
<7>[    0.453809] pci 0000:00:06.0: [106b:003f] type 0 class 0x000c03
<7>[    0.459417] pci 0000:00:06.0: reg 10: [mem 0xf0804000-0xf0804fff]
<7>[    0.470162] pci 0000:00:07.0: [8086:7113] type 0 class 0x000680
<7>[    0.470546] pci 0000:00:0b.0: [8086:265c] type 0 class 0x000c03
<7>[    0.472353] pci 0000:00:0b.0: reg 10: [mem 0xf0805000-0xf0805fff]
<7>[    0.487023] pci 0000:00:0d.0: [8086:2829] type 0 class 0x000106
<7>[    0.488854] pci 0000:00:0d.0: reg 10: [io  0xd240-0xd247]
<7>[    0.496179] pci 0000:00:0d.0: reg 18: [io  0xd250-0xd257]
<7>[    0.500315] pci 0000:00:0d.0: reg 20: [io  0xd260-0xd26f]
<7>[    0.502499] pci 0000:00:0d.0: reg 24: [mem 0xf0806000-0xf0807fff]
<7>[    0.504754] ACPI: PCI Interrupt Routing Table [\_SB_.PCI0._PRT]
<6>[    0.506800] ACPI: PCI Interrupt Link [LNKA] (IRQs 5 9 10 *11)
<6>[    0.506943] ACPI: PCI Interrupt Link [LNKB] (IRQs 5 9 10 *11)
<6>[    0.506992] ACPI: PCI Interrupt Link [LNKC] (IRQs 5 9 *10 11)
<6>[    0.507040] ACPI: PCI Interrupt Link [LNKD] (IRQs 5 *9 10 11)
<6>[    0.507123] vgaarb: device added:
PCI:0000:00:02.0,decodes=io+mem,owns=io+mem,locks=none
<6>[    0.507127] vgaarb: loaded
<5>[    0.507225] SCSI subsystem initialized
<7>[    0.510002] libata version 3.00 loaded.
<6>[    0.510002] usbcore: registered new interface driver usbfs
<6>[    0.510002] usbcore: registered new interface driver hub
<6>[    0.510002] usbcore: registered new device driver usb
<6>[    0.510002] wmi: Mapper loaded
<6>[    0.510002] PCI: Using ACPI for IRQ routing
<7>[    0.510002] PCI: pci_cache_line_size set to 64 bytes
<7>[    0.510002] reserve RAM buffer: 000000000009fc00 - 000000000009ffff
<7>[    0.510002] reserve RAM buffer: 00000000dfff0000 - 00000000dfffffff
<6>[    0.510002] NetLabel: Initializing
<6>[    0.510002] NetLabel:  domain hash size = 128
<6>[    0.510002] NetLabel:  protocols = UNLABELED CIPSOv4
<6>[    0.510002] NetLabel:  unlabeled traffic allowed by default
<6>[    0.516226] AppArmor: AppArmor Filesystem Enabled
<6>[    0.516247] pnp: PnP ACPI init
<6>[    0.516257] ACPI: bus type pnp registered
<7>[    0.516318] pnp 00:00: [bus 00-ff]
<7>[    0.516322] pnp 00:00: [io  0x0cf8-0x0cff]
<7>[    0.516324] pnp 00:00: [io  0x0000-0x0cf7 window]
<7>[    0.516326] pnp 00:00: [io  0x0d00-0xffff window]
<7>[    0.516329] pnp 00:00: [mem 0x000a0000-0x000bffff window]
<7>[    0.516331] pnp 00:00: [mem 0xe0000000-0xffdfffff window]
<7>[    0.516352] pnp 00:00: Plug and Play ACPI device, IDs PNP0a03
(active)
<7>[    0.516368] pnp 00:01: [io  0x0060]
<7>[    0.516370] pnp 00:01: [io  0x0064]
<7>[    0.516396] pnp 00:01: [irq 1]
<7>[    0.516413] pnp 00:01: Plug and Play ACPI device, IDs PNP0303
(active)
<7>[    0.516422] pnp 00:02: [io  0x0000-0x000f]
<7>[    0.516425] pnp 00:02: [io  0x0080-0x008f]
<7>[    0.516427] pnp 00:02: [io  0x00c0-0x00df]
<7>[    0.516430] pnp 00:02: [dma 4]
<7>[    0.516442] pnp 00:02: Plug and Play ACPI device, IDs PNP0200
(active)
<7>[    0.516484] pnp 00:03: [irq 12]
<7>[    0.516501] pnp 00:03: Plug and Play ACPI device, IDs PNP0f03
(active)
<7>[    0.516511] pnp 00:04: [io  0x0378-0x037f]
<7>[    0.516514] pnp 00:04: [io  0x0778-0x077f]
<7>[    0.516528] pnp 00:04: [irq 7]
<7>[    0.516542] pnp 00:04: Plug and Play ACPI device, IDs PNP0400
(active)
<6>[    0.516861] pnp: PnP ACPI: found 5 devices
<6>[    0.516864] ACPI: ACPI bus type pnp unregistered
<6>[    0.522509] Switching to clocksource acpi_pm
<7>[    0.522651] pci_bus 0000:00: resource 0 [io  0x0000-0xffff]
<7>[    0.522654] pci_bus 0000:00: resource 1 [mem 0x00000000-
0xffffffff]
```

```
<6>[    0.522676] NET: Registered protocol family 2
<6>[     0.522753] IP route cache hash table entries: 131072 (order: 8,
1048576 bytes)
<6>[    0.523912] TCP established hash table entries: 524288 (order: 11,
8388608 bytes)
<6>[     0.525678] TCP bind hash table entries: 65536 (order: 8, 1048576
bytes)
<6>[     0.525678] TCP: Hash tables configured (established 524288 bind
65536)
<6>[    0.525678] TCP reno registered
<6>[    0.525686] UDP hash table entries: 2048 (order: 4, 65536 bytes)
<6>[      0.525701] UDP-Lite hash table entries: 2048 (order: 4, 65536
bytes)
<6>[    0.525753] NET: Registered protocol family 1
<6>[    0.525762] pci 0000:00:00.0: Limiting direct PCI/PCI transfers
<6>[    0.525787] pci 0000:00:01.0: Activating ISA DMA hang workarounds
<7>[    0.525807] pci 0000:00:02.0: Boot video device
<7>[    0.525996] PCI: CLS 0 bytes, default 64
<6>[       0.525999] PCI-DMA: Using software bounce buffering for IO
(SWIOTLB)
<6>[    0.526002] Placing 64MB software IO TLB between ffff8800dbc00000 -
ffff8800dfc00000
<6>[    0.526004] software IO TLB at phys 0xdbc00000 - 0xdfc00000
<6>[     0.526106] platform rtc_cmos: registered platform RTC device (no
PNP device found)
<6>[    0.526272] audit: initializing netlink socket (disabled)
<5>[    0.526279] type=2000 audit(1400258836.520:1): initialized
<6>[    0.526085] Switched to NOHz mode on CPU #0
<6>[    0.531022] Switched to NOHz mode on CPU #1
<6>[      0.534722] HugeTLB registered 2 MB page size, pre-allocated 0
pages
<5>[    0.535757] VFS: Disk quotas dquot_6.5.2
<4>[      0.535788] Dquot-cache hash table entries: 512 (order 0, 4096
bytes)
<6>[    0.536162] fuse init (API version 7.16)
<6>[    0.536214] msgmni has been set to 7894
<6>[      0.536416] Block layer SCSI generic (bsg) driver version 0.4
loaded (major 253)
<6>[    0.536448] io scheduler noop registered
<6>[    0.536451] io scheduler deadline registered
<6>[    0.536475] io scheduler cfq registered (default)
<6>[    0.536524] pci_hotplug: PCI Hot Plug PCI Core version: 0.5
<6>[    0.536542] pciehp: PCI Express Hot Plug Controller Driver version:
0.4
<4>[     0.536611] ACPI: Deprecated procfs I/F for AC is loaded, please
retry with CONFIG_ACPI_PROCFS_POWER cleared
<6>[    0.536653] ACPI: AC Adapter [AC] (on-line)
<6>[                      0.536691]     input:     Power     Button     as
/devices/LNXSYSTM:00/LNXPWRBN:00/input/input0
<6>[    0.536694] ACPI: Power Button [PWRF]
<6>[                      0.536735]     input:     Sleep     Button     as
/devices/LNXSYSTM:00/LNXSLPBN:00/input/input1
<6>[    0.536738] ACPI: Sleep Button [SLPF]
<7>[    0.536863] ACPI: acpi_idle registered with cpuidle
<6>[    0.537412] ERST: Table is not found!
<6>[       0.537448] Serial: 8250/16550 driver, 32 ports, IRQ sharing
enabled
<6>[    0.647026] Freeing initrd memory: 12844k freed
<6>[    1.142889] Linux agpgart interface v0.103
<6>[    1.143521] brd: module loaded
<6>[    1.143808] loop: module loaded
<4>[    1.143858] i2c-core: driver [adp5520] using legacy suspend method
<4>[    1.143860] i2c-core: driver [adp5520] using legacy resume method
<7>[    1.143909] ata_piix 0000:00:01.1: version 2.13
<7>[    1.143961] ata_piix 0000:00:01.1: setting latency timer to 64
<6>[    1.144501] scsi0 : ata_piix
<6>[    1.144792] scsi1 : ata_piix
```

```
<6>[    1.144821] ata1: PATA max UDMA/33 cmd 0x1f0 ctl 0x3f6 bmdma 0xd000
irq 14
<6>[    1.144823] ata2: PATA max UDMA/33 cmd 0x170 ctl 0x376 bmdma 0xd008
irq 15
<6>[    1.145054] Fixed MDIO Bus: probed
<6>[    1.145075] PPP generic driver version 2.4.2
<6>[    1.145097] tun: Universal TUN/TAP device driver, 1.6
<6>[    1.145100] tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
<6>[     1.145159] ehci_hcd: USB 2.0 'Enhanced' Host Controller (EHCI)
Driver
<6>[    1.145193] ehci_hcd 0000:00:0b.0: PCI INT A -> GSI 19 (level, low)
-> IRQ 19
<7>[    1.145216] ehci_hcd 0000:00:0b.0: setting latency timer to 64
<6>[    1.145225] ehci_hcd 0000:00:0b.0: EHCI Host Controller
<6>[    1.145250] ehci_hcd 0000:00:0b.0: new USB bus registered, assigned
bus number 1
<6>[    1.150658] ehci_hcd 0000:00:0b.0: irq 19, io mem 0xf0805000
<6>[    1.170157] ehci_hcd 0000:00:0b.0: USB 2.0 started, EHCI 1.00
<6>[    1.170347] hub 1-0:1.0: USB hub found
<6>[    1.170356] hub 1-0:1.0: 8 ports detected
<6>[    1.170537] ohci_hcd: USB 1.1 'Open' Host Controller (OHCI) Driver
<6>[    1.170608] ohci_hcd 0000:00:06.0: PCI INT A -> GSI 22 (level, low)
-> IRQ 22
<7>[    1.170656] ohci_hcd 0000:00:06.0: setting latency timer to 64
<6>[    1.170676] ohci_hcd 0000:00:06.0: OHCI Host Controller
<6>[    1.170734] ohci_hcd 0000:00:06.0: new USB bus registered, assigned
bus number 2
<6>[    1.171026] ohci_hcd 0000:00:06.0: irq 22, io mem 0xf0804000
<6>[    1.230577] hub 2-0:1.0: USB hub found
<6>[    1.230598] hub 2-0:1.0: 8 ports detected
<6>[      1.230866] uhci_hcd: USB Universal Host Controller Interface
driver
<6>[    1.230986] i8042: PNP: PS/2 Controller [PNP0303:PS2K,PNP0f03:PS2M]
at 0x60,0x64 irq 1,12
<6>[    1.235334] serio: i8042 KBD port at 0x60,0x64 irq 1
<6>[    1.235346] serio: i8042 AUX port at 0x60,0x64 irq 12
<6>[    1.235452] mousedev: PS/2 mouse device common for all mice
<6>[         1.235756] input: AT Translated Set 2 keyboard as
/devices/platform/i8042/serio0/input/input2
<6>[     1.236242] rtc_cmos rtc_cmos: rtc core: registered rtc_cmos as
rtc0
<6>[    1.236378] rtc0: alarms up to one day, 114 bytes nvram
<6>[    1.236742] device-mapper: uevent: version 1.0.3
<6>[       1.236850] device-mapper: ioctl: 4.19.1-ioctl (2011-01-07)
initialised: dm-devel@redhat.com
<6>[    1.237860] device-mapper: multipath: version 1.2.0 loaded
<6>[     1.237867] device-mapper: multipath round-robin: version 1.0.0
loaded
<6>[    1.238944] cpuidle: using governor ladder
<6>[    1.238951] cpuidle: using governor menu
<6>[    1.239277] TCP cubic registered
<6>[    1.239451] NET: Registered protocol family 10
<6>[    1.240193] NET: Registered protocol family 17
<5>[    1.240220] Registering the dns_resolver key type
<7>[     1.240482] PM: Hibernation image not present or could not be
loaded.
<4>[    1.240497] registered taskstats version 1
<4>[    1.240956]   Magic number: 14:129:793
<6>[     1.241229] rtc_cmos rtc_cmos: setting system clock to 2014-05-16
16:47:18 UTC (1400258838)
<6>[    1.241249] BIOS EDD facility v0.16 2004-Jun-25, 0 devices found
<6>[    1.241254] EDD information not available.
<6>[    1.301811] ata2.00: ATAPI: VBOX CD-ROM, 1.0, max UDMA/133
<6>[    1.302774] ata2.00: configured for UDMA/33
<5>[     1.303958] scsi 1:0:0:0: CD-ROM                VBOX       CD-ROM
1.0  PQ: 0 ANSI: 5
<4>[    1.305392] sr0: scsi3-mmc drive: 32x/32x xa/form2 tray
<6>[    1.305399] cdrom: Uniform CD-ROM driver Revision: 3.20
```

```
<7>[    1.308170] sr 1:0:0:0: Attached scsi CD-ROM sr0
<5>[    1.309660] sr 1:0:0:0: Attached scsi generic sg0 type 5
<6>[    1.313167] Freeing unused kernel memory: 956k freed
<6>[    1.313303] Write protecting the kernel read-only data: 10240k
<6>[    1.315123] Freeing unused kernel memory: 184k freed
<6>[    1.322403] Freeing unused kernel memory: 1444k freed
<4>[    1.365166] <30>udev[67]: starting version 167
<6>[      1.409547] e1000: Intel(R) PRO/1000 Network Driver - version
7.3.21-k8-NAPI
<6>[    1.409550] e1000: Copyright (c) 1999-2006 Intel Corporation.
<6>[    1.409582] e1000 0000:00:03.0: PCI INT A -> GSI 19 (level, low) ->
IRQ 19
<7>[    1.409598] e1000 0000:00:03.0: setting latency timer to 64
<6>[     1.680131] usb 2-1: new full speed USB device using ohci_hcd and
address 2
<6>[         1.841932]  e1000  0000:00:03.0:  eth0:  (PCI:33MHz:32-bit)
08:00:27:cc:54:b5
<6>[      1.841940] e1000 0000:00:03.0: eth0: Intel(R) PRO/1000 Network
Connection
<7>[    1.842057] ahci 0000:00:0d.0: version 3.0
<6>[    1.842126] ahci 0000:00:0d.0: PCI INT A -> GSI 21 (level, low) ->
IRQ 21
<6>[    1.842233] ahci: SSS flag set, parallel bus scan disabled
<6>[     1.842369] ahci 0000:00:0d.0: AHCI 0001.0100 32 slots 1 ports 3
Gbps 0x1 impl SATA mode
<6>[    1.842376] ahci 0000:00:0d.0: flags: 64bit ncq stag only ccc
<7>[    1.842409] ahci 0000:00:0d.0: setting latency timer to 64
<6>[    1.846574] scsi2 : ahci
<6>[      1.846626] ata3: SATA max UDMA/133 abar m8192@0xf0806000 port
0xf0806100 irq 21
<6>[    2.190315] ata3: SATA link up 3.0 Gbps (SStatus 123 SControl 300)
<6>[    2.190593] ata3.00: ATA-8: VBOX HARDDISK, 1.0, max UDMA/133
<6>[    2.190600] at
[3617576002805444146.3617576002] : USB HID core driver
<6>[    2.268995] SGI XFS with ACLs, security attributes, realtime, large
block/inode numbers, no debug enabled
<6>[    2.275051] SGI XFS Quota Management subsystem
<5>[    2.279154] XFS mounting filesystem sda6
<7>[    2.293333] Ending clean XFS mount for filesystem: sda6
<4>[    2.460259] <30>udev[251]: starting version 167
<6>[       2.470699] Adding 3998716k swap on /dev/sda5.   Priority:-1
extents:1 across:3998716k SS
<6>[    2.533224] lp: driver loaded but no devices found
<6>[     2.606866] EXT4-fs (sda1): mounted filesystem with ordered data
mode. Opts: (null)
<3>[         2.610446]  piix4_smbus  0000:00:07.0:  SMBus  base  address
uninitialized - upgrade BIOS or use force_addr=0xaddr
<6>[     2.617543] pci 0000:00:04.0: PCI INT A -> GSI 20 (level, low) ->
IRQ 20
<6>[                  2.624864]    input:    Unspecified    device    as
/devices/virtual/input/input4
<4>[      2.625339] vboxguest: major 0, IRQ 20, I/O port d020, MMIO at
00000000f0400000 (size 0x400000)
<7>[    2.625352] vboxguest: Successfully loaded version 4.1.8 (interface
0x00010004)
<5>[      2.666314] type=1400 audit(1400258839.911:2): apparmor="STATUS"
operation="profile_load"           name="/sbin/dhclient"           pid=438
comm="apparmor_parser"
<5>[      2.666664] type=1400 audit(1400258839.911:3): apparmor="STATUS"
operation="profile_load"           name="/usr/lib/NetworkManager/nm-dhcp-
client.action" pid=438 comm="apparmor_parser"
<5>[      2.666889] type=1400 audit(1400258839.911:4): apparmor="STATUS"
operation="profile_load"  name="/usr/lib/connman/scripts/dhclient-script"
pid=438 comm="apparmor_parser"
<6>[    2.756745] ADDRCONF(NETDEV_UP): eth0: link is not ready
<6>[     2.760516] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow
Control: RX
<6>[    2.761029] ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
```

```
<6>[    2.763329] parport_pc 00:04: reported by Plug and Play ACPI
<5>[      2.828598] type=1400 audit(1400258840.071:5): apparmor="STATUS"
operation="profile_load"     name="/usr/share/gdm/guest-session/Xsession"
pid=573 comm="apparmor_parser"
<5>[      2.831075] type=1400 audit(1400258840.081:6): apparmor="STATUS"
operation="profile_replace"          name="/sbin/dhclient"          pid=574
comm="apparmor_parser"
<5>[      2.831503] type=1400 audit(1400258840.081:7): apparmor="STATUS"
operation="profile_replace"         name="/usr/lib/NetworkManager/nm-dhcp-
client.action" pid=574 comm="apparmor_parser"
<5>[      2.831724] type=1400 audit(1400258840.081:8): apparmor="STATUS"
operation="profile_replace"       name="/usr/lib/connman/scripts/dhclient-
script" pid=574 comm="apparmor_parser"
<5>[      2.837274] type=1400 audit(1400258840.081:9): apparmor="STATUS"
operation="profile_load"           name="/usr/bin/evince"           pid=576
comm="apparmor_parser"
<5>[     2.837389] type=1400 audit(1400258840.081:10): apparmor="STATUS"
operation="profile_load"   name="/usr/lib/cups/backend/cups-pdf"   pid=578
comm="apparmor_parser"
<6>[         2.849065]  input:  ImExPS/2  Generic  Explorer  Mouse  as
/devices/platform/i8042/serio1/input/input5
<7>[     3.009203] vboxsf: Successfully loaded version 4.1.8 (interface
0x00010004)
<6>[    3.015416] ppdev: user-space parallel port driver
<6>[     3.081070] Intel ICH 0000:00:05.0: PCI INT A -> GSI 21 (level,
low) -> IRQ 21
<7>[    3.081089] Intel ICH 0000:00:05.0: setting latency timer to 64
<6>[    3.168827] EXT4-fs (sda1): re-mounted. Opts: commit=0
<6>[       3.430239]  intel8x0_measure_ac97_clock:  measured  59582  usecs
(12782 samples)
<6>[    3.430246] intel8x0: measured clock 214527 rejected
<6>[       3.800227]  intel8x0_measure_ac97_clock:  measured  59999  usecs
(12774 samples)
<6>[    3.800234] intel8x0: measured clock 212903 rejected
<6>[       4.740268]  intel8x0_measure_ac97_clock:  measured  62047  usecs
(12678 samples)
<6>[    4.740275] intel8x0: measured clock 204328 rejected
<6>[    4.740281] intel8x0: clocking to 48000
<6>[        4.798424]  vesafb:  framebuffer  at  0xe0000000,  mapped  to
0xffffc90004500000, using 1216k, total 1216k
<6>[    4.798429] vesafb: mode is 640x480x32, linelength=2560, pages=0
<6>[    4.798432] vesafb: scrolling: redraw
<6>[    4.798435] vesafb: Truecolor: size=8:8:8:8, shift=24:16:8:0
<4>[    4.798530] Console: switching to colour frame buffer device 80x30
<6>[    4.798541] fb0: VESA VGA frame buffer device
<6>[    4.980466] [drm] Initialized drm 1.1.0 20060810
<6>[     4.981425] pci 0000:00:02.0: PCI INT A -> GSI 18 (level, low) ->
IRQ 18
<7>[    4.981440] pci 0000:00:02.0: setting latency timer to 64
<6>[       4.981546]  [drm]  Supports  vblank  timestamp  caching  Rev  1
(10.10.2010).
<6>[    4.981548] [drm] No driver support for vblank timestamp query.
<6>[       4.981551]  [drm]  Initialized  vboxvideo  1.0.0  20090303  for
0000:00:02.0 on minor 0
<6>[    5.747997] EXT4-fs (sda1): re-mounted. Opts: commit=0
<7>[   13.700173] eth0: no IPv6 routers present
<6>[  192.670530] usb 2-1: USB disconnect, address 2
<6>[  193.200258] usb 2-1: new full speed USB device using ohci_hcd and
address 3
<6>[        193.503032]    input:    VirtualBox    USB    Tablet    as
/devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/input/input6
<6>[  193.503210] generic-usb 0003:80EE:0021.0002: input,hidraw0: USB HID
v1.10 Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
<7>[  224.713621] sf_read_super_aux err=-71
<7>[  224.750645] sf_read_super_aux err=-71
<7>[  224.780382] sf_read_super_aux err=-71
```

B.2 Output for plugin linux_psaux

The output in Table B.1 was generated by the Volatility *linux_psaux* plugin (see Section 3.3.1).

Table B.1: *Plugin output for linux_psaux (sorted by PID).*

PID	UID	GID	Arguments
1	0	0	/sbin/init ro quiet splash
2	0	0	[kthreadd]
3	0	0	[ksoftirqd/0]
5	0	0	[kworker/u:0]
6	0	0	[migration/0]
7	0	0	[migration/1]
9	0	0	[ksoftirqd/1]
10	0	0	[kworker/0:1]
11	0	0	[cpuset]
12	0	0	[khelper]
13	0	0	[netns]
14	0	0	[kworker/u:1]
15	0	0	[sync_supers]
16	0	0	[bdi-default]
17	0	0	[kintegrityd]
18	0	0	[kblockd]
19	0	0	[kacpid]
20	0	0	[kacpi_notify]
21	0	0	[kacpi_hotplug]
22	0	0	[ata_sff]
23	0	0	[khubd]
24	0	0	[md]
25	0	0	[kworker/1:1]
26	0	0	[khungtaskd]
27	0	0	[kswapd0]
28	0	0	[ksmd]
29	0	0	[fsnotify_mark]
30	0	0	[aio]
31	0	0	[ecryptfs-kthrea]
32	0	0	[crypto]
36	0	0	[kthrotld]
38	0	0	[scsi_eh_0]
39	0	0	[scsi_eh_1]
41	0	0	[kmpathd]
42	0	0	[kmpath_handlerd]

PID	UID	GID	Arguments
43	0	0	[kondemand]
44	0	0	[kconservative]
45	0	0	[kworker/0:2]
155	0	0	[kworker/1:2]
166	0	0	[scsi_eh_2]
185	0	0	[xfs_mru_cache]
186	0	0	[xfslogd]
187	0	0	[xfsdatad]
188	0	0	[xfsconvertd]
190	0	0	[xfsbufd/sda6]
191	0	0	[xfsaild/sda6]
192	0	0	[xfssyncd/sda6]
249	0	0	upstart-udev-bridge --daemon
251	0	0	udevd --daemon
370	0	0	[jbd2/sda1-8]
372	0	0	[ext4-dio-unwrit]
405	0	0	[iprt]
406	0	0	[kpsmoused]
420	102	105	dbus-daemon --system --fork --activation=upstart
426	101	103	rsyslogd -c4
444	0	0	NetworkManager
446	104	109	avahi-daemon: ru
447	104	109	avahi-daemon: ch
451	0	0	udevd --daemon
462	0	0	/usr/sbin/modem-manager
467	0	0	/usr/lib/policykit-1/polkitd
522	0	0	/sbin/wpa_supplicant -u -s
523	0	0	/sbin/dhclient -d -4 -sf /usr/lib/NetworkManager/nm-dhcp-client.action -pf /var/run/dhclient-eth0.pid -lf /var/lib/dhcp/dhclient-6cd8b0a6-3c56-4b21-9f2b-6054a5152641-eth0.lease -cf /var/run/nm-dhclient-eth0.conf eth0
562	0	0	upstart-socket-bridge --daemon
621	0	0	/sbin/getty -8 38400 tty4
627	0	0	/sbin/getty -8 38400 tty5
638	0	0	/sbin/getty -8 38400 tty2
641	0	0	/sbin/getty -8 38400 tty3
644	0	0	/sbin/getty -8 38400 tty6
651	0	0	acpid -c /etc/acpi/events -s /var/run/acpid.socket
654	0	0	anacron -s
655	0	0	cron
656	0	0	atd

PID	UID	GID	Arguments
663	0	0	/usr/sbin/irqbalance
787	0	0	/usr/sbin/VBoxService
898	0	0	[flush-8:0]
943	0	0	/sbin/getty -8 38400 tty1
1015	0	0	gdm-binary
1017	0	0	/usr/sbin/cupsd -F
1022	0	0	/usr/sbin/console-kit-daemon --no-daemon
1088	0	0	/usr/lib/gdm/gdm-simple-slave --display-id /org/gnome/DisplayManager/Display1
1091	0	0	/usr/bin/X :0 -br -verbose -auth /var/run/gdm/auth-for-gdm-E6Qm2P/database -nolisten tcp vt7
1136	0	1000	/usr/lib/gdm/gdm-session-worker
1139	0	0	/usr/lib/upower/upowerd
1157	110	119	/usr/lib/rtkit/rtkit-daemon
1233	1000	1000	/usr/bin/gnome-keyring-daemon --daemonize --login
1252	1000	1000	gnome-session --session=ubuntu
1295	1000	1000	/usr/bin/VBoxClient --clipboard
1307	1000	1000	/usr/bin/VBoxClient --display
1315	1000	1000	/usr/bin/VBoxClient --seamless
1319	1000	1000	/usr/bin/ssh-agent /usr/bin/dbus-launch --exit-with-session gnome-session --session=ubuntu
1322	1000	1000	/usr/bin/dbus-launch --exit-with-session gnome-session --session=ubuntu
1323	1000	1000	//bin/dbus-daemon --fork --print-pid 5 --print-address 7 --session
1328	1000	1000	/usr/lib/libgconf2-4/gconfd-2
1344	1000	1000	/usr/lib/gnome-settings-daemon/gnome-settings-daemon
1347	1000	1000	/usr/lib/gvfs/gvfsd
1352	1000	1000	/usr/lib/gvfs//gvfs-fuse-daemon /home/richard/.gvfs
1357	1000	1000	compiz
1359	1000	1000	/usr/bin/pulseaudio --start --log-target=syslog
1362	1000	1000	nautilus
1366	1000	1000	/usr/lib/pulseaudio/pulse/gconf-helper
1370	1000	1000	nm-applet --sm-disable
1371	1000	1000	/usr/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1
1376	1000	1000	/usr/lib/gvfs/gvfs-gdu-volume-monitor
1377	1000	1000	zeitgeist-datahub
1379	0	0	/usr/lib/udisks/udisks-daemon
1381	0	0	udisks-daemon: polling /dev/sr
1386	1000	1000	gnome-power-manager
1392	1000	1000	bluetooth-applet
1397	1000	1000	/usr/bin/python /usr/bin/zeitgeist-daemon

PID	UID	GID	Arguments
1399	1000	1000	/usr/lib/gvfs/gvfs-gphoto2-volume-monitor
1400	1000	1000	/usr/lib/evolution/2.32/evolution-alarm-notify
1402	1000	1000	/usr/lib/gvfs/gvfs-afc-volume-monitor
1419	1000	1000	/bin/cat
1421	1000	1000	[zeitgeist-datah]
1450	1000	1000	/usr/lib/gvfs/gvfsd-trash --spawner :1.10 /org/gtk/gvfs/exec_spaw/0
1454	1000	1000	/usr/lib/notify-osd/notify-osd
1468	1000	1000	/usr/lib/gvfs/gvfsd-metadata
1470	1000	1000	/usr/lib/gvfs/gvfsd-burn --spawner :1.10 /org/gtk/gvfs/exec_spaw/1
1475	1000	1000	/usr/lib/d-conf/dconf-service
1484	1000	1000	/bin/sh -c /usr/bin/compiz-decorator
1485	1000	1000	/usr/bin/unity-window-decorator
1488	1000	1000	/usr/lib/unity/unity-panel-service
1493	1000	1000	/usr/lib/bamf/bamfdaemon
1501	1000	1000	/usr/lib/indicator-datetime/indicator-datetime-service
1502	1000	1000	/usr/lib/indicator-me/indicator-me-service
1503	1000	1000	/usr/lib/indicator-session/indicator-session-service
1504	1000	1000	/usr/lib/indicator-application/indicator-application-service
1505	1000	1000	/usr/lib/indicator-messages/indicator-messages-service
1509	1000	1000	/usr/lib/indicator-sound/indicator-sound-service
1542	1000	1000	/usr/lib/geoclue/geoclue-master
1550	1000	1000	gnome-screensaver
1552	1000	1000	gnome-terminal
1555	1000	1000	gnome-pty-helper
1556	1000	1000	bash
1615	1000	1000	/usr/lib/gnome-disk-utility/gdu-notification-daemon
1618	1000	1000	/usr/bin/python /usr/share/system-config-printer/applet.py
1621	1000	1000	update-notifier
1635	0	0	/usr/bin/python /usr/lib/system-service/system-service-d
1645	1000	1000	/usr/lib/unity-place-applications/unity-applications-daemon
1647	1000	1000	/usr/lib/unity-place-files/unity-files-daemon
1674	0	0	udevd --daemon
1684	0	0	su - root
1692	0	0	-su
1888	0	0	[kworker/0:0]
1889	0	0	[kworker/1:0]

B.3 Output for plugin linux_pslist

The output in Table B.2 was generated by the Volatility *linux_pslist* plugin (see Section 3.3.2).

Table B.2: *Plugin output for linux_pslist (sorted by PID).*

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff8801176b8000	init	1	0	0	0x000000011434d000	2014-05-16 16:47:22 UTC+0000
0xffff8801176b96e0	kthreadd	2	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176badc0	ksoftirqd/0	3	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176bdb80	kworker/u:0	5	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176d8000	migration/0	6	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176d96e0	migration/1	7	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176dc4a0	ksoftirqd/1	9	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176ddb80	kworker/0:1	10	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880117728000	cpuset	11	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801177116e0	khelper	12	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801177296e0	netns	13	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff88011772adc0	kworker/u:1	14	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff88011772c4a0	sync_supers	15	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff88011772db80	bdi-default	16	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880117050000	kintegrityd	17	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801170516e0	kblockd	18	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880117052dc0	kacpid	19	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801170544a0	kacpi_notify	20	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880117055b80	kacpi_hotplug	21	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e48000	ata_sff	22	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e496e0	khubd	23	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e4adc0	md	24	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e4c4a0	kworker/1:1	25	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e4db80	khungtaskd	26	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115ed8000	kswapd0	27	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115ed96e0	ksmd	28	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115edadc0	fsnotify_mark	29	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115edc4a0	aio	30	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115eddb80	ecryptfs-kthrea	31	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115fb8000	crypto	32	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115fbdb80	kthrotld	36	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115fbc4a0	scsi_eh_0	38	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880117712dc0	scsi_eh_1	39	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff8801177144a0	kmpathd	41	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880115fb96e0	kmpath_handlerd	42	0	0	----------	2014-05-16 16:47:23 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff880117715b80	kondemand	43	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880114388000	kconservative	44	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff8801143896e0	kworker/0:2	45	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880113cadb80	kworker/1:2	155	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880113c544a0	scsi_eh_2	166	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880113cac4a0	xfs_mru_cache	185	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113952dc0	xfslogd	186	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff88011438db80	xfsdatad	187	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff8801139516e0	xfsconvertd	188	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff8801139544a0	xfsbufd/sda6	190	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113955b80	xfsaild/sda6	191	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113c55b80	xfssyncd/sda6	192	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113ce8000	upstart-udev-br	249	0	0	0x0000000117157000	2014-05-16 16:47:24 UTC+0000
0xffff880113ddadc0	udevd	251	0	0	0x0000000113938000	2014-05-16 16:47:24 UTC+0000
0xffff8801134044a0	jbd2/sda1-8	370	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113402dc0	ext4-dio-unwrit	372	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880114148000	iprt	405	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff8801141496e0	kpsmoused	406	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880117110000	dbus-daemon	420	102	105	0x0000000114290000	2014-05-16 16:47:24 UTC+0000
0xffff880113e8adc0	rsyslogd	426	101	103	0x0000000113fe9000	2014-05-16 16:47:24 UTC+0000
0xffff880113400000	NetworkManager	444	0	0	0x0000000113654000	2014-05-16 16:47:24 UTC+0000
0xffff880113ca8000	avahi-daemon	446	104	109	0x000000011486d000	2014-05-16 16:47:24 UTC+0000
0xffff88011414db80	avahi-daemon	447	104	109	0x0000000113650000	2014-05-16 16:47:24 UTC+0000
0xffff880114badb80	udevd	451	0	0	0x0000000114801000	2014-05-16 16:47:24 UTC+0000
0xffff88011340adc0	modem-manager	462	0	0	0x0000000114093000	2014-05-16 16:47:24 UTC+0000
0xffff88011583c4a0	polkitd	467	0	0	0x0000000116c90000	2014-05-16 16:47:24 UTC+0000
0xffff8801142244a0	wpa_supplicant	522	0	0	0x000000011136ae000	2014-05-16 16:47:24 UTC+0000
0xffff8801141d2dc0	dhclient	523	0	0	0x0000000114260000	2014-05-16 16:47:24 UTC+0000
0xffff8801141b2dc0	upstart-socket-	562	0	0	0x000000011159e3000	2014-05-16 16:47:24 UTC+0000
0xffff880114182dc0	getty	621	0	0	0x0000000113ba9000	2014-05-16 16:47:24 UTC+0000
0xffff880113c50000	getty	627	0	0	0x000000011348a000	2014-05-16 16:47:24 UTC+0000
0xffff8801141d0000	getty	638	0	0	0x0000000113b94000	2014-05-16 16:47:24 UTC+0000
0xffff8801141d44a0	getty	641	0	0	0x000000011168d2000	2014-05-16 16:47:24 UTC+0000
0xffff880113e8c4a0	getty	644	0	0	0x0000000116f6b000	2014-05-16 16:47:24 UTC+0000
0xffff880113cf0000	acpid	651	0	0	0x0000000113ba0000	2014-05-16 16:47:24 UTC+0000
0xffff880113cf44a0	anacron	654	0	0	0x000000011732c000	2014-05-16 16:47:24 UTC+0000
0xffff880113cf5b80	cron	655	0	0	0x000000011136e6000	2014-05-16 16:47:24 UTC+0000
0xffff8801141b5b80	atd	656	0	0	0x000000011148d6000	2014-05-16 16:47:24 UTC+0000
0xffff880113bc96e0	irqbalance	663	0	0	0x0000000115664000	2014-05-16 16:47:24 UTC+0000
0xffff880113872dc0	VBoxService	787	0	0	0x000000011159a8000	2014-05-16 16:47:25 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff88011414adc0	flush-8:0	898	0	0	----------	2014-05-16 16:47:25 UTC+0000
0xffff880113bc8000	getty	943	0	0	0x000000011406e000	2014-05-16 16:47:25 UTC+0000
0xffff88011583db80	gdm-binary	1015	0	0	0x000000011424b000	2014-05-16 16:47:26 UTC+0000
0xffff8801141d16e0	cupsd	1017	0	0	0x00000001136fe000	2014-05-16 16:47:26 UTC+0000
0xffff880117112dc0	console-kit-dae	1022	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113c516e0	gdm-simple-slav	1088	0	0	0x00000001141c0000	2014-05-16 16:47:26 UTC+0000
0xffff88011352db80	Xorg	1091	0	0	0x00000001171df000	2014-05-16 16:47:26 UTC+0000
0xffff880114ba96e0	gdm-session-wor	1136	0	1000	0x0000000115777000	2014-05-16 16:47:27 UTC+0000
0xffff880114220000	upowerd	1139	0	0	0x0000000115794000	2014-05-16 16:47:27 UTC+0000
0xffff8801157d5b80	rtkit-daemon	1157	110	119	0x0000000114f1d000	2014-05-16 16:47:27 UTC+0000
0xffff880114982dc0	gnome-keyring-d	1233	1000	1000	0x0000000116337000	2014-05-16 16:48:07 UTC+0000
0xffff880114bac4a0	gnome-session	1252	1000	1000	0x0000000114a29000	2014-05-16 16:48:07 UTC+0000
0xffff880114a65b80	VBoxClient	1295	1000	1000	0x0000000114961000	2014-05-16 16:48:08 UTC+0000
0xffff8801149896e0	VBoxClient	1307	1000	1000	0x00000001172e2000	2014-05-16 16:48:08 UTC+0000
0xffff880113bcdb80	VBoxClient	1315	1000	1000	0x00000001148f2000	2014-05-16 16:48:08 UTC+0000
0xffff880114e40000	ssh-agent	1319	1000	1000	0x0000000116ddb000	2014-05-16 16:48:08 UTC+0000
0xffff880113ce96e0	dbus-launch	1322	1000	1000	0x000000011491f000	2014-05-16 16:48:08 UTC+0000
0xffff880113caadc0	dbus-daemon	1323	1000	1000	0x0000000116afd000	2014-05-16 16:48:08 UTC+0000
0xffff8801156c44a0	gconfd-2	1328	1000	1000	0x0000000116da2000	2014-05-16 16:48:08 UTC+0000
0xffff880113870000	gnome-settings-	1344	1000	1000	0x0000000114b08000	2014-05-16 16:48:08 UTC+0000
0xffff880114185b80	gvfsd	1347	1000	1000	0x0000000116d3c000	2014-05-16 16:48:08 UTC+0000
0xffff8801134096e0	gvfs-fuse-daemo	1352	1000	1000	0x0000000116de5000	2014-05-16 16:48:08 UTC+0000
0xffff880114a644a0	compiz	1357	1000	1000	0x0000000115e8f000	2014-05-16 16:48:08 UTC+0000
0xffff8801157d2dc0	pulseaudio	1359	1000	1000	0x00000001172c0000	2014-05-16 16:48:08 UTC+0000
0xffff8801138716e0	nautilus	1362	1000	1000	0x0000000114a01000	2014-05-16 16:48:08 UTC+0000
0xffff88011498adc0	gconf-helper	1366	1000	1000	0x0000000116dd7000	2014-05-16 16:48:08 UTC+0000
0xffff8801172a16e0	nm-applet	1370	1000	1000	0x0000000117118000	2014-05-16 16:48:08 UTC+0000
0xffff880114baadc0	polkit-gnome-au	1371	1000	1000	0x0000000115cf0000	2014-05-16 16:48:08 UTC+0000
0xffff880114f88000	gvfs-gdu-volume	1376	1000	1000	0x0000000116eb6000	2014-05-16 16:48:08 UTC+0000
0xffff880114f896e0	zeitgeist-datah	1377	1000	1000	0x00000001156e9000	2014-05-16 16:48:08 UTC+0000
0xffff88011583adc0	udisks-daemon	1379	0	0	0x00000001156e7000	2014-05-16 16:48:08 UTC+0000
0xffff8801156c0000	udisks-daemon	1381	0	0	0x00000001172ed000	2014-05-16 16:48:08 UTC+0000
0xffff8801171116e0	gnome-power-man	1386	1000	1000	0x0000000115866000	2014-05-16 16:48:08 UTC+0000
0xffff8801138744a0	bluetooth-apple	1392	1000	1000	0x00000001173a4000	2014-05-16 16:48:08 UTC+0000
0xffff880113bcc4a0	zeitgeist-daemo	1397	1000	1000	0x00000001173a6000	2014-05-16 16:48:08 UTC+0000
0xffff880113e88000	gvfs-gphoto2-vo	1399	1000	1000	0x0000000115d28000	2014-05-16 16:48:08 UTC+0000
0xffff8801172a5b80	evolution-alarm	1400	1000	1000	0x0000000113d60000	2014-05-16 16:48:08 UTC+0000
0xffff880115df8000	gvfs-afc-volume	1402	1000	1000	0x0000000115887000	2014-05-16 16:48:08 UTC+0000
0xffff880114a844a0	cat	1419	1000	1000	0x0000000116d05000	2014-05-16 16:48:08 UTC+0000
0xffff880114a816e0	zeitgeist-datah	1421	1000	1000	----------	2014-05-16 16:48:08 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff880115a816e0	gvfsd-trash	1450	1000	1000	0x0000000115a02000	2014-05-16 16:48:09 UTC+0000
0xffff880115a1c4a0	notify-osd	1454	1000	1000	0x0000000115a0f000	2014-05-16 16:48:09 UTC+0000
0xffff880114980000	gvfsd-metadata	1468	1000	1000	0x0000000115bf7000	2014-05-16 16:48:09 UTC+0000
0xffff880115dfc4a0	gvfsd-burn	1470	1000	1000	0x0000000115418000	2014-05-16 16:48:10 UTC+0000
0xffff880113dd8000	dconf-service	1475	1000	1000	0x0000000103dc5000	2014-05-16 16:48:11 UTC+0000
0xffff880113cedb80	sh	1484	1000	1000	0x00000001154dd000	2014-05-16 16:48:11 UTC+0000
0xffff880113ceadc0	unity-window-de	1485	1000	1000	0x0000000115 49a000	2014-05-16 16:48:11 UTC+0000
0xffff880115dfdb80	unity-panel-ser	1488	1000	1000	0x0000000115493000	2014-05-16 16:48:11 UTC+0000
0xffff8801141b0000	bamfdaemon	1493	1000	1000	0x00000001154f3000	2014-05-16 16:48:11 UTC+0000
0xffff880114c20000	indicator-datet	1501	1000	1000	0x0000000114c06000	2014-05-16 16:48:11 UTC+0000
0xffff880114c216e0	indicator-me-se	1502	1000	1000	0x0000000114c68000	2014-05-16 16:48:11 UTC+0000
0xffff880114c22dc0	indicator-sessi	1503	1000	1000	0x00000001155da000	2014-05-16 16:48:11 UTC+0000
0xffff880103d796e0	indicator-appli	1504	1000	1000	0x0000000115 50c000	2014-05-16 16:48:11 UTC+0000
0xffff880103d7adc0	indicator-messa	1505	1000	1000	0x0000000103cec000	2014-05-16 16:48:11 UTC+0000
0xffff880103d7db80	indicator-sound	1509	1000	1000	0x0000000114c78000	2014-05-16 16:48:11 UTC+0000
0xffff880103ea2dc0	geoclue-master	1542	1000	1000	0x0000000103d49000	2014-05-16 16:48:11 UTC+0000
0xffff880103c6c4a0	gnome-screensav	1550	1000	1000	0x0000000103f74000	2014-05-16 16:48:14 UTC+0000
0xffff880103c6adc0	gnome-terminal	1552	1000	1000	0x0000000101558000	2014-05-16 16:48:14 UTC+0000
0xffff880103d7c4a0	gnome-pty-helpe	1555	1000	1000	0x0000000103faf000	2014-05-16 16:48:14 UTC+0000
0xffff880103d78000	bash	1556	1000	1000	0x0000000101 45a000	2014-05-16 16:48:14 UTC+0000
0xffff880103ffdb80	gdu-notificatio	1615	1000	1000	0x0000000103f2c000	2014-05-16 16:48:19 UTC+0000
0xffff880103fe5b80	applet.py	1618	1000	1000	0x0000000116ed2000	2014-05-16 16:48:39 UTC+0000
0xffff880103fe0000	update-notifier	1621	1000	1000	0x0000000036d2a000	2014-05-16 16:49:09 UTC+0000
0xffff880103fe44a0	system-service-	1635	0	0	0x0000000036d18000	2014-05-16 16:49:10 UTC+0000
0xffff880114d82dc0	unity-applicati	1645	1000	1000	0x0000000036d9a000	2014-05-16 16:50:32 UTC+0000
0xffff880114d844a0	unity-files-dae	1647	1000	1000	0x0000000036cf9000	2014-05-16 16:50:32 UTC+0000
0xffff880103e896e0	udevd	1674	0	0	0x0000000036e6e000	2014-05-16 16:50:35 UTC+0000
0xffff8801157d44a0	su	1684	0	0	0x0000000036ee0000	2014-05-16 16:50:38 UTC+0000
0xffff880103ea16e0	bash	1692	0	0	0x0000000036e43000	2014-05-16 16:50:46 UTC+0000
0xffff880103e8db80	kworker/0:0	1888	0	0	----------	2014-05-16 16:52:25 UTC+0000
0xffff880103fe16e0	kworker/1:0	1889	0	0	----------	2014-05-16 16:52:27 UTC+0000

B.4 Output for plugin linux_pstree

The output in Table B.3 was generated by the Volatility *linux_pslist* plugin (see Section 3.3.4).

Table B.3: *Plugin output for linux_pstree (dot levels indicate subprocess).*

Name	PID	UID
init	1	0
.upstart-udev-br	249	0
.udevd	251	0
..udevd	451	0
..udevd	1674	0
.dbus-daemon	420	102
.rsyslogd	426	101
.NetworkManager	444	0
..dhclient	523	0
.avahi-daemon	446	104
..avahi-daemon	447	104
.modem-manager	462	0
.polkitd	467	0
.wpa_supplicant	522	0
.upstart-socket-	562	0
.getty	621	0
.getty	627	0
.getty	638	0
.getty	641	0
.getty	644	0
.acpid	651	0
.anacron	654	0
.cron	655	0
.atd	656	0
.irqbalance	663	0
.VBoxService	787	0
.getty	943	0
.gdm-binary	1015	0
..gdm-simple-slav	1088	0
...Xorg	1091	0
...gdm-session-wor	1136	0
....gnome-session	1252	1000
.....ssh-agent	1319	1000
.....compiz	1357	1000
......sh	1484	1000

Name	PID	UID
.......unity-window-de	1485	1000
.....nautilus	1362	1000
.....nm-applet	1370	1000
.....polkit-gnome-au	1371	1000
.....zeitgeist-datah	1377	1000
.....gnome-power-man	1386	1000
.....bluetooth-apple	1392	1000
.....evolution-alarm	1400	1000
.....gdu-notificatio	1615	1000
.....applet.py	1618	1000
.....update-notifier	1621	1000
.cupsd	1017	0
.console-kit-dae	1022	0
.upowerd	1139	0
.rtkit-daemon	1157	110
.gnome-keyring-d	1233	1000
.VBoxClient	1295	1000
.VBoxClient	1307	1000
.VBoxClient	1315	1000
.dbus-daemon	1323	1000
.dbus-launch	1322	1000
.gconfd-2	1328	1000
.gvfsd	1347	1000
.gvfs-fuse-daemo	1352	1000
.gnome-settings-	1344	1000
.pulseaudio	1359	1000
..gconf-helper	1366	1000
.udisks-daemon	1379	0
..udisks-daemon	1381	0
.gvfs-gdu-volume	1376	1000
.gvfs-gphoto2-vo	1399	1000
.gvfs-afc-volume	1402	1000
.zeitgeist-daemo	1397	1000
..cat	1419	1000
..[zeitgeist-datah]	1421	1000
.gvfsd-trash	1450	1000
.notify-osd	1454	1000
.gvfsd-metadata	1468	1000
.gvfsd-burn	1470	1000
.dconf-service	1475	1000

Name	PID	UID
.bamfdaemon	1493	1000
.unity-panel-ser	1488	1000
.indicator-messa	1505	1000
.indicator-appli	1504	1000
.indicator-datet	1501	1000
.indicator-me-se	1502	1000
.indicator-sessi	1503	1000
.geoclue-master	1542	1000
.indicator-sound	1509	1000
.gnome-screensav	1550	1000
.gnome-terminal	1552	1000
..gnome-pty-helpe	1555	1000
..bash	1556	1000
...su	1684	0
....bash	1692	0
.system-service-	1635	0
.unity-files-dae	1647	1000
.unity-applicati	1645	1000
[kthreadd]	2	0
.[ksoftirqd/0]	3	0
.[kworker/u:0]	5	0
.[migration/0]	6	0
.[migration/1]	7	0
.[ksoftirqd/1]	9	0
.[kworker/0:1]	10	0
.[cpuset]	11	0
.[khelper]	12	0
.[netns]	13	0
.[kworker/u:1]	14	0
.[sync_supers]	15	0
.[bdi-default]	16	0
.[kintegrityd]	17	0
.[kblockd]	18	0
.[kacpid]	19	0
.[kacpi_notify]	20	0
.[kacpi_hotplug]	21	0
.[ata_sff]	22	0
.[khubd]	23	0
.[md]	24	0
.[kworker/1:1]	25	0

Name	PID	UID
.[khungtaskd]	26	0
.[kswapd0]	27	0
.[ksmd]	28	0
.[fsnotify_mark]	29	0
.[aio]	30	0
.[ecryptfs-kthrea]	31	0
.[crypto]	32	0
.[kthrotld]	36	0
.[scsi_eh_0]	38	0
.[scsi_eh_1]	39	0
.[kmpathd]	41	0
.[kmpath_handlerd]	42	0
.[kondemand]	43	0
.[kconservative]	44	0
.[kworker/0:2]	45	0
.[kworker/1:2]	155	0
.[scsi_eh_2]	166	0
.[xfs_mru_cache]	185	0
.[xfslogd]	186	0
.[xfsdatad]	187	0
.[xfsconvertd]	188	0
.[xfsbufd/sda6]	190	0
.[xfsaild/sda6]	191	0
.[xfssyncd/sda6]	192	0
.[jbd2/sda1-8]	370	0
.[ext4-dio-unwrit]	372	0
.[iprt]	405	0
.[kpsmoused]	406	0
.[flush-8:0]	898	0
.[kworker/0:0]	1888	0
.[kworker/1:0]	1889	0

B.5 Output for plugin linux_pidhashtable

The output in Table B.4 was generated by the Volatility *linux_pidhashtable* plugin (see Section 3.3.5).

Table B.4: *Plugin output for linux_pidhashtable (sorted by PID).*

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff8801176b8000	init	1	0	0	0x000000011434d000	2014-05-16 16:47:22 UTC+0000
0xffff8801176b96e0	kthreadd	2	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176badc0	ksoftirqd/0	3	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176bdb80	kworker/u:0	5	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176d8000	migration/0	6	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176d96e0	migration/1	7	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176dc4a0	ksoftirqd/1	9	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801176ddb80	kworker/0:1	10	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880117728000	cpuset	11	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801177116e0	khelper	12	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801177296e0	netns	13	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff88011772adc0	kworker/u:1	14	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff88011772c4a0	sync_supers	15	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff88011772db80	bdi-default	16	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880117050000	kintegrityd	17	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801170516e0	kblockd	18	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880117052dc0	kacpid	19	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff8801170544a0	kacpi_notify	20	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880117055b80	kacpi_hotplug	21	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e48000	ata_sff	22	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e496e0	khubd	23	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e4adc0	md	24	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e4c4a0	kworker/1:1	25	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880116e4db80	khungtaskd	26	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115ed8000	kswapd0	27	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115ed96e0	ksmd	28	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115edadc0	fsnotify_mark	29	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115edc4a0	aio	30	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115eddb80	ecryptfs-kthrea	31	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115fb8000	crypto	32	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115fbdb80	kthrotld	36	0	0	----------	2014-05-16 16:47:22 UTC+0000
0xffff880115fbc4a0	scsi_eh_0	38	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880117712dc0	scsi_eh_1	39	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff8801177144a0	kmpathd	41	0	0	----------	2014-05-16 16:47:23 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff880115fb96e0	kmpath_handlerd	42	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880117715b80	kondemand	43	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880114388000	kconservative	44	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff8801143896e0	kworker/0:2	45	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880113cadb80	kworker/1:2	155	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880113c544a0	scsi_eh_2	166	0	0	----------	2014-05-16 16:47:23 UTC+0000
0xffff880113cac4a0	xfs_mru_cache	185	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113952dc0	xfslogd	186	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff88011438db80	xfsdatad	187	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff8801139516e0	xfsconvertd	188	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff8801139544a0	xfsbufd/sda6	190	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113955b80	xfsaild/sda6	191	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113c55b80	xfssyncd/sda6	192	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113ce8000	upstart-udev-br	249	0	0	0x0000000117157000	2014-05-16 16:47:24 UTC+0000
0xffff880113ddadc0	udevd	251	0	0	0x0000000113938000	2014-05-16 16:47:24 UTC+0000
0xffff8801134044a0	jbd2/sda1-8	370	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880113402dc0	ext4-dio-unwrit	372	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880114148000	iprt	405	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff8801141496e0	kpsmoused	406	0	0	----------	2014-05-16 16:47:24 UTC+0000
0xffff880117110000	dbus-daemon	420	102	105	0x0000000114290000	2014-05-16 16:47:24 UTC+0000
0xffff880113e8adc0	rsyslogd	426	101	103	0x0000000113fe9000	2014-05-16 16:47:24 UTC+0000
0xffff880114edc4a0	rsyslogd	441	101	103	0x0000000113fe9000	2014-05-16 16:47:24 UTC+0000
0xffff8801156c5b80	rsyslogd	442	101	103	0x0000000113fe9000	2014-05-16 16:47:24 UTC+0000
0xffff880113400000	NetworkManager	444	0	0	0x0000000113654000	2014-05-16 16:47:24 UTC+0000
0xffff880113ca8000	avahi-daemon	446	104	109	0x000000011486d000	2014-05-16 16:47:24 UTC+0000
0xffff88011414db80	avahi-daemon	447	104	109	0x0000000113650000	2014-05-16 16:47:24 UTC+0000
0xffff880114badb80	udevd	451	0	0	0x0000000114801000	2014-05-16 16:47:24 UTC+0000
0xffff88011340adc0	modem-manager	462	0	0	0x0000000114093000	2014-05-16 16:47:24 UTC+0000
0xffff88011438c4a0	NetworkManager	463	0	0	0x0000000113654000	2014-05-16 16:47:24 UTC+0000
0xffff88011583c4a0	polkitd	467	0	0	0x0000000116c90000	2014-05-16 16:47:24 UTC+0000
0xffff8801171144a0	polkitd	469	0	0	0x0000000116c90000	2014-05-16 16:47:24 UTC+0000
0xffff8801142244a0	wpa_supplicant	522	0	0	0x00000001136ae000	2014-05-16 16:47:24 UTC+0000
0xffff8801141d2dc0	dhclient	523	0	0	0x0000000114260000	2014-05-16 16:47:24 UTC+0000
0xffff880114225b80	NetworkManager	524	0	0	0x0000000113654000	2014-05-16 16:47:24 UTC+0000
0xffff8801141b2dc0	upstart-socket-	562	0	0	0x00000001159e3000	2014-05-16 16:47:24 UTC+0000
0xffff880114182dc0	getty	621	0	0	0x0000000113ba9000	2014-05-16 16:47:24 UTC+0000
0xffff880113c50000	getty	627	0	0	0x000000011348a000	2014-05-16 16:47:24 UTC+0000
0xffff8801141d0000	getty	638	0	0	0x0000000113b94000	2014-05-16 16:47:24 UTC+0000
0xffff8801141d44a0	getty	641	0	0	0x00000001168d2000	2014-05-16 16:47:24 UTC+0000
0xffff880113e8c4a0	getty	644	0	0	0x0000000116f6b000	2014-05-16 16:47:24 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff880113cf0000	acpid	651	0	0	0x0000000113ba0000	2014-05-16 16:47:24 UTC+0000
0xffff880113cf44a0	anacron	654	0	0	0x000000011732c000	2014-05-16 16:47:24 UTC+0000
0xffff880113cf5b80	cron	655	0	0	0x00000001136e6000	2014-05-16 16:47:24 UTC+0000
0xffff8801141b5b80	atd	656	0	0	0x00000001148d6000	2014-05-16 16:47:24 UTC+0000
0xffff880113bc96e0	irqbalance	663	0	0	0x0000000115664000	2014-05-16 16:47:24 UTC+0000
0xffff880113872dc0	VBoxService	787	0	0	0x00000001159a8000	2014-05-16 16:47:25 UTC+0000
0xffff880114e18000	VBoxService	789	0	0	0x00000001159a8000	2014-05-16 16:47:25 UTC+0000
0xffff880114e196e0	VBoxService	790	0	0	0x00000001159a8000	2014-05-16 16:47:25 UTC+0000
0xffff880114e1db80	VBoxService	791	0	0	0x00000001159a8000	2014-05-16 16:47:25 UTC+0000
0xffff880114e1c4a0	VBoxService	792	0	0	0x00000001159a8000	2014-05-16 16:47:25 UTC+0000
0xffff880114e444a0	VBoxService	793	0	0	0x00000001159a8000	2014-05-16 16:47:25 UTC+0000
0xffff880114e45b80	VBoxService	794	0	0	0x00000001159a8000	2014-05-16 16:47:25 UTC+0000
0xffff8801158144a0	VBoxService	795	0	0	0x00000001159a8000	2014-05-16 16:47:25 UTC+0000
0xffff88011414adc0	flush-8:0	898	0	0	----------	2014-05-16 16:47:25 UTC+0000
0xffff880113bc8000	getty	943	0	0	0x000000011406e000	2014-05-16 16:47:25 UTC+0000
0xffff88011583db80	gdm-binary	1015	0	0	0x000000011424b000	2014-05-16 16:47:26 UTC+0000
0xffff8801141d16e0	cupsd	1017	0	0	0x00000001136fe000	2014-05-16 16:47:26 UTC+0000
0xffff880117112dc0	console-kit-dae	1022	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114222dc0	console-kit-dae	1023	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801134016e0	console-kit-dae	1024	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801141b44a0	console-kit-dae	1025	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801141b16e0	console-kit-dae	1026	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114ed96e0	console-kit-dae	1027	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114edadc0	console-kit-dae	1028	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114ed8000	console-kit-dae	1029	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113408000	console-kit-dae	1030	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113ca96e0	console-kit-dae	1031	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113cec4a0	console-kit-dae	1032	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e1adc0	console-kit-dae	1033	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113cf16e0	console-kit-dae	1034	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e42dc0	console-kit-dae	1035	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e416e0	console-kit-dae	1036	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113e8db80	console-kit-dae	1037	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880115815b80	console-kit-dae	1038	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880115812dc0	console-kit-dae	1039	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113bcadc0	console-kit-dae	1040	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113c52dc0	console-kit-dae	1041	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113dddb80	console-kit-dae	1042	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880115600000	console-kit-dae	1043	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801156016e0	console-kit-dae	1044	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff880115602dc0	console-kit-dae	1045	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801156044a0	console-kit-dae	1046	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880115605b80	console-kit-dae	1047	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e70000	console-kit-dae	1048	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e716e0	console-kit-dae	1049	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e72dc0	console-kit-dae	1050	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e744a0	console-kit-dae	1051	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e75b80	console-kit-dae	1052	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e78000	console-kit-dae	1053	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e796e0	console-kit-dae	1054	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e7adc0	console-kit-dae	1055	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e7c4a0	console-kit-dae	1056	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880114e7db80	console-kit-dae	1057	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113500000	console-kit-dae	1058	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801135016e0	console-kit-dae	1059	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113502dc0	console-kit-dae	1060	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801135044a0	console-kit-dae	1061	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113505b80	console-kit-dae	1062	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113508000	console-kit-dae	1063	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801135096e0	console-kit-dae	1064	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff88011350adc0	console-kit-dae	1065	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff88011350c4a0	console-kit-dae	1066	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff88011350db80	console-kit-dae	1067	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113510000	console-kit-dae	1068	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801135116e0	console-kit-dae	1069	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113512dc0	console-kit-dae	1070	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801135144a0	console-kit-dae	1071	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113515b80	console-kit-dae	1072	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113518000	console-kit-dae	1073	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801135196e0	console-kit-dae	1074	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff88011351adc0	console-kit-dae	1075	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff88011351c4a0	console-kit-dae	1076	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff88011351db80	console-kit-dae	1077	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113520000	console-kit-dae	1078	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801135216e0	console-kit-dae	1079	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113522dc0	console-kit-dae	1080	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801135244a0	console-kit-dae	1081	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113525b80	console-kit-dae	1082	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113528000	console-kit-dae	1083	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff8801135296e0	console-kit-dae	1084	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff880114eddb80	console-kit-dae	1086	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113cf2dc0	console-kit-dae	1087	0	0	0x000000011425f000	2014-05-16 16:47:26 UTC+0000
0xffff880113c516e0	gdm-simple-slav	1088	0	0	0x00000001141c0000	2014-05-16 16:47:26 UTC+0000
0xffff88011352c4a0	gdm-binary	1089	0	0	0x000000011424b000	2014-05-16 16:47:26 UTC+0000
0xffff88011352db80	Xorg	1091	0	0	0x00000001171df000	2014-05-16 16:47:26 UTC+0000
0xffff88011352adc0	gdm-simple-slav	1092	0	0	0x00000001141c0000	2014-05-16 16:47:26 UTC+0000
0xffff880114ba96e0	gdm-session-wor	1136	0	1000	0x0000000115777000	2014-05-16 16:47:27 UTC+0000
0xffff880114220000	upowerd	1139	0	0	0x0000000115794000	2014-05-16 16:47:27 UTC+0000
0xffff8801141d5b80	upowerd	1142	0	0	0x0000000115794000	2014-05-16 16:47:27 UTC+0000
0xffff8801157d5b80	rtkit-daemon	1157	110	119	0x0000000114f1d000	2014-05-16 16:47:27 UTC+0000
0xffff880114f8c4a0	rtkit-daemon	1162	110	119	0x0000000114f1d000	2014-05-16 16:47:27 UTC+0000
0xffff880114f8db80	rtkit-daemon	1163	110	119	0x0000000114f1d000	2014-05-16 16:47:27 UTC+0000
0xffff880114982dc0	gnome-keyring-d	1233	1000	1000	0x0000000116337000	2014-05-16 16:48:07 UTC+0000
0xffff880114a62dc0	gnome-keyring-d	1234	1000	1000	0x0000000116337000	2014-05-16 16:48:07 UTC+0000
0xffff880114bac4a0	gnome-session	1252	1000	1000	0x0000000114a29000	2014-05-16 16:48:07 UTC+0000
0xffff880113dd96e0	gdm-session-wor	1253	0	1000	0x0000000115777000	2014-05-16 16:48:07 UTC+0000
0xffff880114a65b80	VBoxClient	1295	1000	1000	0x0000000114961000	2014-05-16 16:48:08 UTC+0000
0xffff880114a60000	VBoxClient	1299	1000	1000	0x0000000114961000	2014-05-16 16:48:08 UTC+0000
0xffff8801149896e0	VBoxClient	1307	1000	1000	0x00000001172e2000	2014-05-16 16:48:08 UTC+0000
0xffff8801142216e0	VBoxClient	1312	1000	1000	0x00000001172e2000	2014-05-16 16:48:08 UTC+0000
0xffff880113bcdb80	VBoxClient	1315	1000	1000	0x00000001148f2000	2014-05-16 16:48:08 UTC+0000
0xffff8801158396e0	VBoxClient	1316	1000	1000	0x00000001148f2000	2014-05-16 16:48:08 UTC+0000
0xffff880114e40000	ssh-agent	1319	1000	1000	0x0000000116ddb000	2014-05-16 16:48:08 UTC+0000
0xffff880113ce96e0	dbus-launch	1322	1000	1000	0x000000011491f000	2014-05-16 16:48:08 UTC+0000
0xffff880113caadc0	dbus-daemon	1323	1000	1000	0x0000000116afd000	2014-05-16 16:48:08 UTC+0000
0xffff880115810000	gnome-session	1326	1000	1000	0x0000000114a29000	2014-05-16 16:48:08 UTC+0000
0xffff8801156c44a0	gconfd-2	1328	1000	1000	0x0000000116da2000	2014-05-16 16:48:08 UTC+0000
0xffff8801158116e0	gnome-session	1330	1000	1000	0x0000000114a29000	2014-05-16 16:48:08 UTC+0000
0xffff880117115b80	gnome-keyring-d	1339	1000	1000	0x0000000116337000	2014-05-16 16:48:08 UTC+0000
0xffff880113405b80	gnome-keyring-d	1341	1000	1000	0x0000000116337000	2014-05-16 16:48:08 UTC+0000
0xffff8801141816e0	gnome-keyring-d	1343	1000	1000	0x0000000116337000	2014-05-16 16:48:08 UTC+0000
0xffff880113870000	gnome-settings-	1344	1000	1000	0x0000000114b08000	2014-05-16 16:48:08 UTC+0000
0xffff880114180000	gnome-settings-	1345	1000	1000	0x0000000114b08000	2014-05-16 16:48:08 UTC+0000
0xffff880114185b80	gvfsd	1347	1000	1000	0x0000000116d3c000	2014-05-16 16:48:08 UTC+0000
0xffff8801134096e0	gvfs-fuse-daemo	1352	1000	1000	0x0000000116de5000	2014-05-16 16:48:08 UTC+0000
0xffff88011340c4a0	gvfs-fuse-daemo	1353	1000	1000	0x0000000116de5000	2014-05-16 16:48:08 UTC+0000
0xffff88011340db80	gvfs-fuse-daemo	1354	1000	1000	0x0000000116de5000	2014-05-16 16:48:08 UTC+0000
0xffff880114a616e0	gvfs-fuse-daemo	1355	1000	1000	0x0000000116de5000	2014-05-16 16:48:08 UTC+0000
0xffff880114a644a0	compiz	1357	1000	1000	0x0000000115e8f000	2014-05-16 16:48:08 UTC+0000
0xffff8801157d2dc0	pulseaudio	1359	1000	1000	0x00000001172c0000	2014-05-16 16:48:08 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff880113875b80	compiz	1360	1000	1000	0x0000000115e8f000	2014-05-16 16:48:08 UTC+0000
0xffff8801157d16e0	alsa-sink	1361	1000	1000	0x00000001172c0000	2014-05-16 16:48:08 UTC+0000
0xffff8801138716e0	nautilus	1362	1000	1000	0x0000000114a01000	2014-05-16 16:48:08 UTC+0000
0xffff8801157d0000	alsa-source	1363	1000	1000	0x00000001172c0000	2014-05-16 16:48:08 UTC+0000
0xffff88011498adc0	gconf-helper	1366	1000	1000	0x0000000116dd7000	2014-05-16 16:48:08 UTC+0000
0xffff8801172a2dc0	gconf-helper	1367	1000	1000	0x0000000116dd7000	2014-05-16 16:48:08 UTC+0000
0xffff8801172a16e0	nm-applet	1370	1000	1000	0x0000000117118000	2014-05-16 16:48:08 UTC+0000
0xffff880114baadc0	polkit-gnome-au	1371	1000	1000	0x0000000115cf0000	2014-05-16 16:48:08 UTC+0000
0xffff880114f88000	gvfs-gdu-volume	1376	1000	1000	0x0000000116eb6000	2014-05-16 16:48:08 UTC+0000
0xffff880114f896e0	zeitgeist-datah	1377	1000	1000	0x00000001156e9000	2014-05-16 16:48:08 UTC+0000
0xffff88011583adc0	udisks-daemon	1379	0	0	0x00000001156e7000	2014-05-16 16:48:08 UTC+0000
0xffff8801156c0000	udisks-daemon	1381	0	0	0x00000001172ed000	2014-05-16 16:48:08 UTC+0000
0xffff8801156c16e0	udisks-daemon	1385	0	0	0x00000001156e7000	2014-05-16 16:48:08 UTC+0000
0xffff8801171116e0	gnome-power-man	1386	1000	1000	0x0000000115866000	2014-05-16 16:48:08 UTC+0000
0xffff8801141844a0	zeitgeist-datah	1389	1000	1000	0x00000001156e9000	2014-05-16 16:48:08 UTC+0000
0xffff8801138744a0	bluetooth-apple	1392	1000	1000	0x00000001173a4000	2014-05-16 16:48:08 UTC+0000
0xffff8801156c2dc0	polkit-gnome-au	1393	1000	1000	0x0000000115cf0000	2014-05-16 16:48:08 UTC+0000
0xffff880113bcc4a0	zeitgeist-daemo	1397	1000	1000	0x00000001173a6000	2014-05-16 16:48:08 UTC+0000
0xffff880113e88000	gvfs-gphoto2-vo	1399	1000	1000	0x0000000115d28000	2014-05-16 16:48:08 UTC+0000
0xffff8801172a5b80	evolution-alarm	1400	1000	1000	0x0000000113d60000	2014-05-16 16:48:08 UTC+0000
0xffff880115df8000	gvfs-afc-volume	1402	1000	1000	0x0000000115887000	2014-05-16 16:48:08 UTC+0000
0xffff880115df96e0	gvfs-afc-volume	1403	1000	1000	0x0000000115887000	2014-05-16 16:48:08 UTC+0000
0xffff880114a82dc0	nautilus	1406	1000	1000	0x0000000114a01000	2014-05-16 16:48:08 UTC+0000
0xffff880113e896e0	nm-applet	1411	1000	1000	0x0000000117118000	2014-05-16 16:48:08 UTC+0000
0xffff880115dfadc0	gnome-power-man	1416	1000	1000	0x0000000115866000	2014-05-16 16:48:08 UTC+0000
0xffff880114a844a0	cat	1419	1000	1000	0x0000000116d05000	2014-05-16 16:48:08 UTC+0000
0xffff880114a85b80	zeitgeist-daemo	1420	1000	1000	0x00000001173a6000	2014-05-16 16:48:08 UTC+0000
0xffff880115a58000	bluetooth-apple	1447	1000	1000	0x00000001173a4000	2014-05-16 16:48:09 UTC+0000
0xffff880115a816e0	gvfsd-trash	1450	1000	1000	0x0000000115a02000	2014-05-16 16:48:09 UTC+0000
0xffff880115a80000	bluetooth-apple	1453	1000	1000	0x00000001173a4000	2014-05-16 16:48:09 UTC+0000
0xffff880115a1c4a0	notify-osd	1454	1000	1000	0x0000000115a0f000	2014-05-16 16:48:09 UTC+0000
0xffff880115a844a0	evolution-alarm	1457	1000	1000	0x0000000113d60000	2014-05-16 16:48:09 UTC+0000
0xffff880115a85b80	notify-osd	1460	1000	1000	0x0000000115a0f000	2014-05-16 16:48:09 UTC+0000
0xffff880114980000	gvfsd-metadata	1468	1000	1000	0x0000000115bf7000	2014-05-16 16:48:09 UTC+0000
0xffff880115dfc4a0	gvfsd-burn	1470	1000	1000	0x0000000115418000	2014-05-16 16:48:10 UTC+0000
0xffff880113ddc4a0	compiz	1472	1000	1000	0x0000000115e8f000	2014-05-16 16:48:10 UTC+0000
0xffff880113dd8000	dconf-service	1475	1000	1000	0x0000000103dc5000	2014-05-16 16:48:11 UTC+0000
0xffff880115a5c4a0	dconf-service	1477	1000	1000	0x0000000103dc5000	2014-05-16 16:48:11 UTC+0000
0xffff880113cedb80	sh	1484	1000	1000	0x00000001154dd000	2014-05-16 16:48:11 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff880113ceadc0	unity-window-de	1485	1000	1000	0x000000011549a000	2014-05-16 16:48:11 UTC+0000
0xffff880115dfdb80	unity-panel-ser	1488	1000	1000	0x0000000115493000	2014-05-16 16:48:11 UTC+0000
0xffff880115a1adc0	unity-window-de	1489	1000	1000	0x000000011549a000	2014-05-16 16:48:11 UTC+0000
0xffff880115a5db80	unity-panel-ser	1491	1000	1000	0x0000000115493000	2014-05-16 16:48:11 UTC+0000
0xffff8801141b0000	bamfdaemon	1493	1000	1000	0x00000001154f3000	2014-05-16 16:48:11 UTC+0000
0xffff880115a5adc0	unity-panel-ser	1495	1000	1000	0x0000000115493000	2014-05-16 16:48:11 UTC+0000
0xffff880114c20000	indicator-datet	1501	1000	1000	0x0000000114c06000	2014-05-16 16:48:11 UTC+0000
0xffff880114c216e0	indicator-me-se	1502	1000	1000	0x0000000114c68000	2014-05-16 16:48:11 UTC+0000
0xffff880114c22dc0	indicator-sessi	1503	1000	1000	0x00000001155da000	2014-05-16 16:48:11 UTC+0000
0xffff880103d796e0	indicator-appli	1504	1000	1000	0x000000011550c000	2014-05-16 16:48:11 UTC+0000
0xffff880103d7adc0	indicator-messa	1505	1000	1000	0x0000000103cec000	2014-05-16 16:48:11 UTC+0000
0xffff880103d7db80	indicator-sound	1509	1000	1000	0x0000000114c78000	2014-05-16 16:48:11 UTC+0000
0xffff880114d80000	indicator-appli	1515	1000	1000	0x000000011550c000	2014-05-16 16:48:11 UTC+0000
0xffff880114d816e0	indicator-messa	1516	1000	1000	0x0000000103cec000	2014-05-16 16:48:11 UTC+0000
0xffff880114d85b80	indicator-datet	1523	1000	1000	0x0000000114c06000	2014-05-16 16:48:11 UTC+0000
0xffff880103e244a0	indicator-me-se	1531	1000	1000	0x0000000114c68000	2014-05-16 16:48:11 UTC+0000
0xffff880103e8adc0	indicator-datet	1538	1000	1000	0x0000000114c06000	2014-05-16 16:48:11 UTC+0000
0xffff880103c6db80	indicator-sessi	1539	1000	1000	0x00000001155da000	2014-05-16 16:48:11 UTC+0000
0xffff880103ea0000	indicator-sound	1540	1000	1000	0x0000000114c78000	2014-05-16 16:48:11 UTC+0000
0xffff880103ea2dc0	geoclue-master	1542	1000	1000	0x0000000103d49000	2014-05-16 16:48:11 UTC+0000
0xffff880103ea44a0	geoclue-master	1543	1000	1000	0x0000000103d49000	2014-05-16 16:48:11 UTC+0000
0xffff880103e8c4a0	indicator-sound	1544	1000	1000	0x0000000114c78000	2014-05-16 16:48:11 UTC+0000
0xffff880103c6c4a0	gnome-screensav	1550	1000	1000	0x0000000103f74000	2014-05-16 16:48:14 UTC+0000
0xffff880103c6adc0	gnome-terminal	1552	1000	1000	0x0000000101558000	2014-05-16 16:48:14 UTC+0000
0xffff880103c68000	gnome-terminal	1554	1000	1000	0x0000000101558000	2014-05-16 16:48:14 UTC+0000
0xffff880103d7c4a0	gnome-pty-helpe	1555	1000	1000	0x0000000103faf000	2014-05-16 16:48:14 UTC+0000
0xffff880103d78000	bash	1556	1000	1000	0x000000010145a000	2014-05-16 16:48:14 UTC+0000
0xffff880103e88000	gnome-terminal	1557	1000	1000	0x0000000101558000	2014-05-16 16:48:14 UTC+0000
0xffff880103ffdb80	gdu-notificatio	1615	1000	1000	0x0000000103f2c000	2014-05-16 16:48:19 UTC+0000
0xffff880103fe5b80	applet.py	1618	1000	1000	0x0000000116ed2000	2014-05-16 16:48:39 UTC+0000
0xffff880103fe0000	update-notifier	1621	1000	1000	0x0000000036d2a000	2014-05-16 16:49:09 UTC+0000
0xffff880103ff8000	update-notifier	1622	1000	1000	0x0000000036d2a000	2014-05-16 16:49:09 UTC+0000
0xffff880103fe44a0	system-service-	1635	0	0	0x0000000036d18000	2014-05-16 16:49:10 UTC+0000
0xffff880114d82dc0	unity-applicati	1645	1000	1000	0x0000000036d9a000	2014-05-16 16:50:32 UTC+0000
0xffff880114d844a0	unity-files-dae	1647	1000	1000	0x0000000036cf9000	2014-05-16 16:50:32 UTC+0000
0xffff880115838000	unity-files-dae	1648	1000	1000	0x0000000036cf9000	2014-05-16 16:50:32 UTC+0000
0xffff8801149844a0	unity-applicati	1649	1000	1000	0x0000000036d9a000	2014-05-16 16:50:32 UTC+0000
0xffff880103e896e0	udevd	1674	0	0	0x0000000036e6e000	2014-05-16 16:50:35 UTC+0000
0xffff8801157d44a0	su	1684	0	0	0x0000000036ee0000	2014-05-16 16:50:38 UTC+0000
0xffff880103ea16e0	bash	1692	0	0	0x0000000036e43000	2014-05-16 16:50:46 UTC+0000

Offset	Name	PID	UID	GID	DTB	Start Time
0xffff880103e8db80	kworker/0:0	1888	0	0	----------	2014-05-16 16:52:25 UTC+0000
0xffff880103fe16e0	kworker/1:0	1889	0	0	----------	2014-05-16 16:52:27 UTC+0000
0xffff8801156788b8	**?GQ???**	**2800**	**14135 67809**	**39...7**	**0x0000000000000000**	**2014-05-16 16:47:22 UTC+0000**

B.6 Output for plugin linux_psxview

The output in Table B.5 was generated by the Volatility *linux_psxview* plugin (see Section 3.3.6).

Table B.5: *Plugin output for linux_psxview (sorted by PID).*

Offset(V)	Name	PID	Pslist	Pid_hash	Kmem_cache	Parents	Leaders
0x0000000000000000	----------	-----	FALSE	FALSE	FALSE	FALSE	TRUE
0xffffffff81a0b020	swapper	0	FALSE	FALSE	FALSE	TRUE	FALSE
0xffff8801176b8000	init	1	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff8801176b96e0	kthreadd	2	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff8801176badc0	ksoftirqd/0	3	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801176bdb80	kworker/u:0	5	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801176d8000	migration/0	6	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801176d96e0	migration/1	7	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801176dc4a0	ksoftirqd/1	9	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801176ddb80	kworker/0:1	10	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880117728000	cpuset	11	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801177116e0	khelper	12	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801177296e0	netns	13	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011772adc0	kworker/u:1	14	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011772c4a0	sync_supers	15	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011772db80	bdi-default	16	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880117050000	kintegrityd	17	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801170516e0	kblockd	18	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880117052dc0	kacpid	19	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801170544a0	kacpi_notify	20	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880117055b80	kacpi_hotplug	21	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880116e48000	ata_sff	22	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880116e496e0	khubd	23	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880116e4adc0	md	24	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880116e4c4a0	kworker/1:1	25	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880116e4db80	khungtaskd	26	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115ed8000	kswapd0	27	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115ed96e0	ksmd	28	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115edadc0	fsnotify_mark	29	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115edc4a0	aio	30	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115eddb80	ecryptfs-kthrea	31	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115fb8000	crypto	32	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115fbdb80	kthrotld	36	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115fbc4a0	scsi_eh_0	38	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880117712dc0	scsi_eh_1	39	TRUE	TRUE	FALSE	FALSE	TRUE

Offset(V)	Name	PID	Pslist	Pid_hash	Kmem_cache	Parents	Leaders
0xffff8801177144a0	kmpathd	41	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115fb96e0	kmpath_handlerd	42	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880117715b80	kondemand	43	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114388000	kconservative	44	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801143896e0	kworker/0:2	45	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113cadb80	kworker/1:2	155	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113c544a0	scsi_eh_2	166	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113cac4a0	xfs_mru_cache	185	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113952dc0	xfslogd	186	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011438db80	xfsdatad	187	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801139516e0	xfsconvertd	188	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801139544a0	xfsbufd/sda6	190	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113955b80	xfsaild/sda6	191	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113c55b80	xfssyncd/sda6	192	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113ce8000	upstart-udev-br	249	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113ddadc0	udevd	251	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff8801134044a0	jbd2/sda1-8	370	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113402dc0	ext4-dio-unwrit	372	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114148000	iprt	405	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801141496e0	kpsmoused	406	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880117110000	dbus-daemon	420	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113e8adc0	rsyslogd	426	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114edc4a0	rsyslogd	441	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801156c5b80	rsyslogd	442	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113400000	NetworkManager	444	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff880113ca8000	avahi-daemon	446	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff88011414db80	avahi-daemon	447	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114badb80	udevd	451	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011340adc0	modem-manager	462	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011438c4a0	NetworkManager	463	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011583c4a0	polkitd	467	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801171144a0	polkitd	469	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801142244a0	wpa_supplicant	522	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801141d2dc0	dhclient	523	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114225b80	NetworkManager	524	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801141b2dc0	upstart-socket-	562	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114182dc0	getty	621	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113c50000	getty	627	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801141d0000	getty	638	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801141d44a0	getty	641	TRUE	TRUE	FALSE	FALSE	TRUE

Offset(V)	Name	PID	Pslist	Pid_hash	Kmem_cache	Parents	Leaders
0xffff880113e8c4a0	getty	644	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113cf0000	acpid	651	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113cf44a0	anacron	654	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113cf5b80	cron	655	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801141b5b80	atd	656	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113bc96e0	irqbalance	663	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113872dc0	VBoxService	787	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114e18000	VBoxService	789	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e196e0	VBoxService	790	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e1db80	VBoxService	791	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e1c4a0	VBoxService	792	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e444a0	VBoxService	793	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e45b80	VBoxService	794	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801158144a0	VBoxService	795	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011414adc0	flush-8:0	898	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113bc8000	getty	943	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011583db80	gdm-binary	1015	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff8801141d16e0	cupsd	1017	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880117112dc0	console-kit-dae	1022	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114222dc0	console-kit-dae	1023	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801134016e0	console-kit-dae	1024	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801141b44a0	console-kit-dae	1025	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801141b16e0	console-kit-dae	1026	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114ed96e0	console-kit-dae	1027	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114edadc0	console-kit-dae	1028	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114ed8000	console-kit-dae	1029	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113408000	console-kit-dae	1030	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113ca96e0	console-kit-dae	1031	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113cec4a0	console-kit-dae	1032	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e1adc0	console-kit-dae	1033	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113cf16e0	console-kit-dae	1034	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e42dc0	console-kit-dae	1035	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e416e0	console-kit-dae	1036	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113e8db80	console-kit-dae	1037	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115815b80	console-kit-dae	1038	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115812dc0	console-kit-dae	1039	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113bcadc0	console-kit-dae	1040	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113c52dc0	console-kit-dae	1041	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113dddb80	console-kit-dae	1042	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115600000	console-kit-dae	1043	FALSE	TRUE	FALSE	FALSE	FALSE

Offset(V)	Name	PID	Pslist	Pid_hash	Kmem_cache	Parents	Leaders
0xffff8801156016e0	console-kit-dae	1044	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115602dc0	console-kit-dae	1045	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801156044a0	console-kit-dae	1046	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115605b80	console-kit-dae	1047	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e70000	console-kit-dae	1048	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e716e0	console-kit-dae	1049	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e72dc0	console-kit-dae	1050	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e744a0	console-kit-dae	1051	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e75b80	console-kit-dae	1052	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e78000	console-kit-dae	1053	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e796e0	console-kit-dae	1054	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e7adc0	console-kit-dae	1055	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e7c4a0	console-kit-dae	1056	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e7db80	console-kit-dae	1057	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113500000	console-kit-dae	1058	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801135016e0	console-kit-dae	1059	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113502dc0	console-kit-dae	1060	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801135044a0	console-kit-dae	1061	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113505b80	console-kit-dae	1062	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113508000	console-kit-dae	1063	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801135096e0	console-kit-dae	1064	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011350adc0	console-kit-dae	1065	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011350c4a0	console-kit-dae	1066	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011350db80	console-kit-dae	1067	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113510000	console-kit-dae	1068	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801135116e0	console-kit-dae	1069	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113512dc0	console-kit-dae	1070	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801135144a0	console-kit-dae	1071	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113515b80	console-kit-dae	1072	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113518000	console-kit-dae	1073	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801135196e0	console-kit-dae	1074	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011351adc0	console-kit-dae	1075	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011351c4a0	console-kit-dae	1076	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011351db80	console-kit-dae	1077	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113520000	console-kit-dae	1078	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801135216e0	console-kit-dae	1079	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113522dc0	console-kit-dae	1080	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801135244a0	console-kit-dae	1081	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113525b80	console-kit-dae	1082	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113528000	console-kit-dae	1083	FALSE	TRUE	FALSE	FALSE	FALSE

Offset(V)	Name	PID	Pslist	Pid_hash	Kmem_cache	Parents	Leaders
0xffff8801135296e0	console-kit-dae	1084	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114eddb80	console-kit-dae	1086	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113cf2dc0	console-kit-dae	1087	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113c516e0	gdm-simple-slav	1088	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff88011352c4a0	gdm-binary	1089	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011352db80	Xorg	1091	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011352adc0	gdm-simple-slav	1092	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114ba96e0	gdm-session-wor	1136	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff880114220000	upowerd	1139	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801141d5b80	upowerd	1142	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801157d5b80	rtkit-daemon	1157	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114f8c4a0	rtkit-daemon	1162	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114f8db80	rtkit-daemon	1163	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114982dc0	gnome-keyring-d	1233	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114a62dc0	gnome-keyring-d	1234	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114bac4a0	gnome-session	1252	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff880113dd96e0	gdm-session-wor	1253	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114a65b80	VBoxClient	1295	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114a60000	VBoxClient	1299	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801149896e0	VBoxClient	1307	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801142216e0	VBoxClient	1312	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113bcdb80	VBoxClient	1315	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801158396e0	VBoxClient	1316	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114e40000	ssh-agent	1319	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113ce96e0	dbus-launch	1322	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113caadc0	dbus-daemon	1323	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115810000	gnome-session	1326	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801156c44a0	gconfd-2	1328	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801158116e0	gnome-session	1330	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880117115b80	gnome-keyring-d	1339	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113405b80	gnome-keyring-d	1341	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801141816e0	gnome-keyring-d	1343	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113870000	gnome-settings-	1344	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114180000	gnome-settings-	1345	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114185b80	gvfsd	1347	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801134096e0	gvfs-fuse-daemo	1352	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011340c4a0	gvfs-fuse-daemo	1353	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011340db80	gvfs-fuse-daemo	1354	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114a616e0	gvfs-fuse-daemo	1355	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114a644a0	compiz	1357	TRUE	TRUE	FALSE	TRUE	TRUE

Offset(V)	Name	PID	Pslist	Pid_hash	Kmem_cache	Parents	Leaders
0xffff8801157d2dc0	pulseaudio	1359	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff880113875b80	compiz	1360	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801157d16e0	alsa-sink	1361	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801138716e0	nautilus	1362	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801157d0000	alsa-source	1363	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff88011498adc0	gconf-helper	1366	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801172a2dc0	gconf-helper	1367	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801172a16e0	nm-applet	1370	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114baadc0	polkit-gnome-au	1371	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114f88000	gvfs-gdu-volume	1376	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114f896e0	zeitgeist-datah	1377	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff88011583adc0	udisks-daemon	1379	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff8801156c0000	udisks-daemon	1381	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801156c16e0	udisks-daemon	1385	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801171116e0	gnome-power-man	1386	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801141844a0	zeitgeist-datah	1389	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801138744a0	bluetooth-apple	1392	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801156c2dc0	polkit-gnome-au	1393	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113bcc4a0	zeitgeist-daemo	1397	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff880113e88000	gvfs-gphoto2-vo	1399	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801172a5b80	evolution-alarm	1400	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115df8000	gvfs-afc-volume	1402	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115df96e0	gvfs-afc-volume	1403	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114a82dc0	nautilus	1406	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113e896e0	nm-applet	1411	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115dfadc0	gnome-power-man	1416	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114a844a0	cat	1419	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114a85b80	zeitgeist-daemo	1420	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114a816e0	zeitgeist-datah	1421	TRUE	FALSE	FALSE	FALSE	FALSE
0xffff880115a58000	bluetooth-apple	1447	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115a816e0	gvfsd-trash	1450	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115a80000	bluetooth-apple	1453	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115a1c4a0	notify-osd	1454	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115a844a0	evolution-alarm	1457	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115a85b80	notify-osd	1460	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114980000	gvfsd-metadata	1468	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115dfc4a0	gvfsd-burn	1470	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880113ddc4a0	compiz	1472	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113dd8000	dconf-service	1475	TRUE	TRUE	FALSE	FALSE	TRUE

Offset(V)	Name	PID	Pslist	Pid_hash	Kmem_cache	Parents	Leaders
0xffff880115a5c4a0	dconf-service	1477	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880113cedb80	sh	1484	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff880113ceadc0	unity-window-de	1485	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115dfdb80	unity-panel-ser	1488	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115a1adc0	unity-window-de	1489	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880115a5db80	unity-panel-ser	1491	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801141b0000	bamfdaemon	1493	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115a5adc0	unity-panel-ser	1495	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114c20000	indicator-datet	1501	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114c216e0	indicator-me-se	1502	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114c22dc0	indicator-sessi	1503	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103d796e0	indicator-appli	1504	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103d7adc0	indicator-messa	1505	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103d7db80	indicator-sound	1509	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114d80000	indicator-appli	1515	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114d816e0	indicator-messa	1516	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880114d85b80	indicator-datet	1523	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103e244a0	indicator-me-se	1531	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103e8adc0	indicator-datet	1538	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103c6db80	indicator-sessi	1539	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103ea0000	indicator-sound	1540	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103ea2dc0	geoclue-master	1542	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103ea44a0	geoclue-master	1543	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103e8c4a0	indicator-sound	1544	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103c6c4a0	gnome-screensav	1550	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103c6adc0	gnome-terminal	1552	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff880103c68000	gnome-terminal	1554	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103d7c4a0	gnome-pty-helpe	1555	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103d78000	bash	1556	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff880103e88000	gnome-terminal	1557	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103ffdb80	gdu-notificatio	1615	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103fe5b80	applet.py	1618	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103fe0000	update-notifier	1621	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103ff8000	update-notifier	1622	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103fe44a0	system-service-	1635	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114d82dc0	unity-applicati	1645	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880114d844a0	unity-files-dae	1647	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880115838000	unity-files-dae	1648	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff8801149844a0	unity-applicati	1649	FALSE	TRUE	FALSE	FALSE	FALSE
0xffff880103e896e0	udevd	1674	TRUE	TRUE	FALSE	FALSE	TRUE

Offset(V)	Name	PID	Pslist	Pid_hash	Kmem_cache	Parents	Leaders
0xffff8801157d44a0	su	1684	TRUE	TRUE	FALSE	TRUE	TRUE
0xffff880103ea16e0	bash	1692	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103e8db80	kworker/0:0	1888	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff880103fe16e0	kworker/1:0	1889	TRUE	TRUE	FALSE	FALSE	TRUE
0xffff8801156788b8	?GQ???	2800	FALSE	TRUE	FALSE	FALSE	FALSE

B.7 Output for plugin linux_lsmod

The output in Table B.6 was generated by the Volatility *linux_lsmod* plugin (see Section 3.6.1).

Table B.6: *Plugin output for linux_lsmod (sorted by base address).*

Base Address	Kernel Module	Size in Memory (in bytes)
ffffffffa0279380	vboxvideo	12540
ffffffffa02abd20	drm	227495
ffffffffa027f1a0	vesafb	13761
ffffffffa023a140	binfmt_misc	17565
ffffffffa0272740	snd_intel8x0	38272
ffffffffa0262680	snd_ac97_codec	134270
ffffffffa0244080	ac97_bus	12730
ffffffffa022e520	snd_pcm	96625
ffffffffa0210040	snd_seq_midi	13324
ffffffffa0218080	snd_rawmidi	30486
ffffffffa014b020	snd_seq_midi_event	14899
ffffffffa0209700	vboxsf	39343
ffffffffa01cc060	ppdev	17113
ffffffffa01fb280	snd_seq	61621
ffffffffa01eb0a0	snd_timer	29602
ffffffffa01af060	snd_seq_device	14462
ffffffffa01530a0	joydev	17606
ffffffffa01442c0	parport_pc	36959
ffffffffa01de260	snd	67382
ffffffffa01c2e20	psmouse	73535
ffffffffa015a100	serio_raw	13166
ffffffffa000b000	soundcore	12680
ffffffffa01959c0	vboxguest	232904
ffffffffa015fb00	i2c_piix4	13303
ffffffffa0041040	snd_page_alloc	18529
ffffffffa0139080	lp	17825
ffffffffa016c380	parport	46458
ffffffffa010c6e0	xfs	823190
ffffffffa002e000	exportfs	12998

Base Address	Kernel Module	Size in Memory (in bytes)
ffffffffa00662a0	usbhid	46956
ffffffffa0056c80	hid	91020
ffffffffa003aa80	ahci	25951
ffffffffa00259a0	e1000	111862
ffffffffa0004300	libahci	26642

B.8 Output for plugin linux_check_fop

The output in Table B.7 was generated by the Volatility *linux_check_fop* plugin (see Section 3.6.5).

Table B.7: *Plugin output for linux_check_fop (sorted by Symbol Name).*

Symbol Name	Member	Address
/	readdir	0xffffffffa02bd020
/	readdir	0xffffffffa02bd000
/bin	readdir	0xffffffffa02bd020
/boot	readdir	0xffffffffa02bd020
/dev	readdir	0xffffffffa02bd020
/etc	readdir	0xffffffffa02bd020
/etc/avahi	readdir	0xffffffffa02bd020
/etc/cron.d	readdir	0xffffffffa02bd020
/etc/X11	readdir	0xffffffffa02bd020
/etc/xdg	readdir	0xffffffffa02bd020
/etc/xdg/menus	readdir	0xffffffffa02bd020
/home	readdir	0xffffffffa02bd020
/home/richard	readdir	0xffffffffa02bd020
/home/richard/.cache	readdir	0xffffffffa02bd020
/home/richard/.cache/dconf	readdir	0xffffffffa02bd020
/home/richard/.cache/zeitgeist	readdir	0xffffffffa02bd020
/home/richard/.config	readdir	0xffffffffa02bd020
/home/richard/.config/dconf	readdir	0xffffffffa02bd020
/home/richard/.gvfs	readdir	0xffffffffa02bd020
/home/richard/.local	readdir	0xffffffffa02bd020
/home/richard/.local...zeitgeist/fts.index	readdir	0xffffffffa02bd020
/home/richard/.local/share	readdir	0xffffffffa02bd020
/home/richard/.local/share/gvfs-metadata	readdir	0xffffffffa02bd020
/home/richard/.local/share/zeitgeist	readdir	0xffffffffa02bd020
/home/richard/.pulse	readdir	0xffffffffa02bd020
/lib	readdir	0xffffffffa02bd020
/lib/modules	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/auxdisplay	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/block/drbd	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-.../drivers/char/mwave	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/hid/usbhid	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/i2c/busses	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/infiniband	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/input/misc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/isdn/hisax	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/isdn/hysdn	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/isdn/mISDN	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/misc/cb710	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/misc/ti-st	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/net/arcnet	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/net/e1000e	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/net/netxen	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/net/pcmcia	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/net/qlcnic	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/net/stmmac	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/scsi/bnx2i	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/scsi/cxgbi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/scsi/libfc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/scsi/mvsas	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/staging/hv	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/tty/serial	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/usb/c67x00	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/usb/gadget	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/usb/serial	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/video/kyro	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/video/riva	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/w1/masters	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../drivers/xen/xenbus	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../infiniband/hw/mlx4	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../infiniband/ulp/srp	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/cpu/cpufreq	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/ata	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/atm	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-.../kernel/drivers/dca	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/dma	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/gpu	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/hid	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/i2c	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/mfd	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/mmc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/mtd	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/net	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/nfc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/pci	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/pps	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/rtc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/spi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/ssb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/tty	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/uio	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/usb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/uwb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/drivers/xen	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/fs/configfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/fs/exportfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/fs/freevxfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/fs/reiserfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/fs/squashfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/sound/synth	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../kernel/ubuntu/aufs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../media/dvb/dvb-core	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../media/dvb/firewire	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../media/radio/si470x	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../media/video/au0828	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../media/video/em28xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../net/bluetooth/bnep	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../net/bluetooth/cmtp	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-.../net/bluetooth/hidp	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../net/ipv4/netfilter	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../net/ipv6/netfilter	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../net/netfilter/ipvs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../sound/drivers/opl3	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../sound/drivers/pcsp	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../sound/pci/korg1212	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../sound/pci/lx6464es	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../staging/quickstart	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../staging/serqt_usb2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../staging/vme/boards	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../staging/wlags49_h2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../ubuntu/iscsitarget	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../ubuntu/ndiswrapper	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../usb/misc/sisusbvga	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../wireless/ath/ath5k	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../wireless/ath/ath9k	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-.../wireless/b43legacy	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...6/kernel/cpu/mcheck	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...a/video/gspca/gl860	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...a/video/gspca/m5602	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...arch/x86/kernel/cpu	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/drivers/md	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/drivers/w1	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/fs/autofs4	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/fs/fscache	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/fs/hfsplus	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/net/bridge	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/net/decnet	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/net/econet	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/net/netrom	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/net/phonet	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/net/sunrpc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...c/kernel/sound/core	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...dia/video/usbvision	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/char/pcmcia	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/gpu/drm/i2c	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/gpu/drm/mga	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/gpu/drm/sis	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/gpu/drm/ttm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/gpu/drm/via	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/input/mouse	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/input/serio	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/isdn/divert	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/media/radio	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/media/video	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/message/i2o	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/misc/c2port	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/misc/eeprom	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/misc/ibmasm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/mtd/devices	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/mtd/onenand	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/net/bonding	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/net/can/usb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/net/chelsio	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/net/cxgb4vf	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/net/ixgbevf	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/net/pch_gbe	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/net/vmxnet3	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/net/wan/lmc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/pci/hotplug	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/pps/clients	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/scsi/arcmsr	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/scsi/libsas	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/scsi/pcmcia	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/scsi/pm8001	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/staging/bcm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/staging/iio	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...drivers/staging/sep	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/staging/vme	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/usb/storage	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...drivers/video/geode	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...edia/video/et61x251	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/char/agp	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/char/ip2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/char/tpm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/dma/ioat	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/firewire	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/firmware	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/gpu/stub	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/isdn/i4l	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/media/rc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/memstick	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/mmc/card	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/mmc/host	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/mtd/maps	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/mtd/nand	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/net/atlx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/net/caif	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/net/enic	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/net/irda	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/net/ixgb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/net/mlx4	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/net/qlge	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/net/skfp	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/net/vxge	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/platform	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/scsi/bfa	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/scsi/osd	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/usb/host	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/usb/misc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/drivers/watchdog	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...el/fs/ocfs2/cluster	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/lib/reed_solomon	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/lib/zlib_deflate	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/drivers/vx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/pci/asihpi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/pci/au88x0	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/pci/ca0106	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/pci/cs46xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/pci/mixart	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/pci/oxygen	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/pci/ymfpci	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/soc/codecs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/sound/synth/emux	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/ubuntu/compcache	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...el/ubuntu/rtl8192se	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/drivers	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/adfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/affs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/befs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/ceph	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/cifs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/coda	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/fuse	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/gfs2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/hpfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/nfsd	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/ntfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/omfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/qnx4	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/fs/sysv	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/net/802	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/net/atm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/net/can	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/net/ipx	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...eric/kernel/net/key	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/net/llc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/net/rds	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...eric/kernel/net/x25	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/drivers/block	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/drivers/hwmon	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/drivers/input	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/drivers/media	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/drivers/power	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/drivers/vhost	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/drivers/video	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/fs/cachefiles	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/fs/nfs_common	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/net/appletalk	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/net/bluetooth	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/net/netfilter	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/net/wanrouter	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/security/keys	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/sound/drivers	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/sound/pci/aw2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/sound/pci/hda	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ernel/ubuntu/rfkill	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/gpu/drm/nouveau	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/infiniband/core	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/media/dvb/bt8xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/media/dvb/ngene	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/media/dvb/siano	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/media/dvb/ttpci	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/media/video/pwc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/media/video/uvc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/net/can/sja1000	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/net/can/softing	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/cx25821	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/easycap	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...ers/staging/iio/adc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/iio/dac	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/iio/dds	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/iio/imu	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/rtl8712	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/slicoss	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/speakup	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/winbond	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/staging/wlan-ng	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/video/backlight	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ers/video/vermilion	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ess/rtl818x/rtl8180	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ess/rtl818x/rtl8187	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...et/bluetooth/rfcomm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...et/bridge/netfilter	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...et/decnet/netfilter	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...et/wireless/ipw2x00	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...et/wireless/iwlwifi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...et/wireless/orinoco	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...et/wireless/prism54	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...et/wireless/rtl818x	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...et/wireless/rtlwifi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...g/comedi/kcomedilib	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...g/ft1000/ft1000-usb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ging/comedi/drivers	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ging/samsung-laptop	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ia/dvb/ttusb-budget	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/fs/cramfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/fs/nilfs2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/lib/raid6	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/net/8021q	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/net/rxrpc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/net/sched	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/net/wimax	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...ic/kernel/sound/i2c	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/sound/isa	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/sound/pci	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/sound/soc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ic/kernel/sound/usb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...infiniband/hw/cxgb3	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...infiniband/hw/cxgb4	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...infiniband/hw/ipath	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...infiniband/hw/mthca	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...infiniband/ulp/iser	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...iniband/hw/amso1100	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ireless/libertas_tf	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...isdn/hardware/eicon	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...isdn/hardware/mISDN	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/infiniband/hw	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/isdn/hardware	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/media/dvb/pt1	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/memstick/core	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/memstick/host	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/net/appletalk	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/net/tokenring	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/scsi/be2iscsi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/scsi/megaraid	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/staging/keucr	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/staging/line6	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/staging/panel	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/staging/se401	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/staging/sm7xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/staging/smbfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/staging/ti-st	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/staging/usbip	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/staging/xgifb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/usb/host/whci	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/uwb/i1480/dfu	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...ivers/video/display	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/video/intelfb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ivers/video/mb862xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/arch/x86/kvm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/drivers/acpi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/drivers/char	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/drivers/edac	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/drivers/gpio	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/drivers/idle	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/drivers/isdn	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/drivers/leds	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/drivers/misc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/drivers/scsi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/fs/ocfs2/dlm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/net/mac80211	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/net/wireless	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/sound/isa/sb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...kernel/sound/pcmcia	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/arch/x86/oprofile	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/acpi/apei	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/block/aoe	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/bluetooth	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/char/ipmi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/i2c/algos	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/i2c/muxes	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/isdn/capi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/media/dvb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/mtd/chips	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/mtd/lpddr	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/mtd/tests	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/atl1c	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/atl1e	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/benet	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/bnx2x	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...l/drivers/net/cxgb3	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/cxgb4	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/e1000	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/igbvf	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/ixgbe	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/tulip	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/net/wimax	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/regulator	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/scsi/fcoe	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/scsi/fnic	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/scsi/lpfc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/telephony	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/usb/class	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/usb/image	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/uwb/i1480	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/video/aty	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/video/sis	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/video/via	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/w1/slaves	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/drivers/xen/xenfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/sound/pci/ali5451	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/sound/pci/emu10k1	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/sound/pci/ice1712	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/sound/pci/riptide	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/sound/pci/rme9652	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/sound/pci/trident	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...l/ubuntu/dm-raid4-5	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/common/tuners	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/dvb/frontends	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/dvb/ttusb-dec	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/video/cx231xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/video/cx23885	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/video/cx25840	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/video/pvrusb2	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...media/video/saa7134	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/video/saa7164	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/video/sn9c102	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...media/video/tlg2300	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nd/pcmcia/pdaudiocf	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/arch/x86/crypto	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/arch/x86/kernel	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/crypto/async_tx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/gpu/drm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/message	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/mtd/ubi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/net/bna	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/net/can	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/net/igb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/net/phy	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/net/sfc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/net/usb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/net/wan	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/parport	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/staging	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/usb/atm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/drivers/usb/otg	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/net/irda/ircomm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/sound/i2c/other	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/sound/pci/ctxfi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/sound/pci/nm256	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/sound/pci/pcxhr	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/sound/pci/vx222	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/sound/pcmcia/vx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/sound/usb/caiaq	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/sound/usb/usx2y	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/ubuntu/fsam7400	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nel/ubuntu/omnibook	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/crypto	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...neric/kernel/fs/afs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/bfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/dlm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/efs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/fat	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/hfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/jfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/nfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/nls	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/udf	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/ufs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/fs/xfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/lib/xz	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/net/9p	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...neric/kernel/ubuntu	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...net/sunrpc/auth_gss	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...net/sunrpc/xprtrdma	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...net/wireless/hostap	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...net/wireless/rt2x00	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...net/wireless/wl1251	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...net/wireless/wl12xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...nfiniband/ulp/ipoib	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ng/iio/magnetometer	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ound/drivers/mpu401	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...put/joystick/iforce	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...r/pcmcia/ipwireless	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...reless/ath/carl9170	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...reless/iwmc3200wifi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/arch/x86	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/btrfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/exofs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/isofs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/jffs2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/lockd	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...ric/kernel/fs/minix	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/ncpfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/ocfs2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/quota	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/romfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/fs/ubifs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/ax25	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/caif	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/ceph	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/core	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/dccp	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/ipv4	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/ipv6	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/irda	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/l2tp	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/lapb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/rose	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/sctp	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/tipc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/net/xfrm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...ric/kernel/security	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/block/paride	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/gpu/drm/i810	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/gpu/drm/i830	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/gpu/drm/i915	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/gpu/drm/r128	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/gpu/drm/tdfx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/input/tablet	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/isdn/gigaset	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/media/common	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/net/hamradio	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/net/myri10ge	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/net/wireless	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/platform/x86	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...rivers/scsi/aacraid	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/scsi/aic7xxx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/scsi/aic94xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/scsi/mpt2sas	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/scsi/qla2xxx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/scsi/qla4xxx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/staging/echo	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/staging/lirc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/staging/zram	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/usb/wusbcore	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/video/matrox	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/video/nvidia	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rivers/video/savage	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/drivers/crypto	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/drivers/pcmcia	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/drivers/target	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/drivers/virtio	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/fs/ocfs2/dlmfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/net/batman-adv	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/net/ieee802154	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/net/irda/irlan	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/net/irda/irnet	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/sound/core/seq	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/sound/pci/ac97	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rnel/sound/usb/misc	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/media/dvb/dm1105	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/media/dvb/mantis	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/media/dvb/pluto2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/media/rc/keymaps	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/media/video/cx18	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/media/video/cx88	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/media/video/ivtv	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/misc/iwmc3200top	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/net/wimax/i2400m	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...rs/net/wireless/ath	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/net/wireless/b43	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/net/wireless/p54	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/scsi/sym53c8xx_2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/staging/cptm1217	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/staging/frontier	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/staging/iio/gyro	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/staging/pohmelfs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/staging/rtl8192e	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/staging/rtl8192u	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/staging/ste_rmi4	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...rs/staging/usbvideo	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/infiniband/hw/qib	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/input/touchscreen	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/isdn/hardware/avm	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/media/dvb/dvb-usb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/media/video/bt8xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/media/video/cpia2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/media/video/gspca	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/media/video/hdpvr	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/media/video/zoran	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/rtlwifi/rtl8192ce	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/scsi/cxgbi/cxgb3i	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/scsi/cxgbi/cxgb4i	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/asus_oled	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/brcm80211	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/crystalhd	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/dt3155v4l	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/iio/accel	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/iio/addac	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/iio/light	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/iio/meter	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/rtl8187se	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...s/staging/rts_pstor	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...s/staging/sbe-2t3e3	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...scsi/device_handler	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...sound/pci/echoaudio	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...staging/iio/trigger	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...staging/vme/bridges	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...staging/vme/devices	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...staging/wlags49_h25	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...t/wireless/libertas	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...t/wireless/zd1211rw	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...taging/iio/resolver	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...taging/quatech_usb2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...und/pci/cs5535audio	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/char/hw_random	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/gpu/drm/radeon	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/gpu/drm/savage	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/infiniband/ulp	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/input/gameport	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/input/joystick	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/input/keyboard	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/media/dvb/b2c2	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/message/fusion	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/autofs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/comedi	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/cxt1e1	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/dabusb	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/et131x	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/ft1000	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/go7007	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/phison	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/rt2860	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/rt2870	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/tm6000	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/staging/vt6656	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...vers/tty/serial/jsm	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/lib/modules/2.6.38-...video/gspca/stv06xx	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-...wireless/ath/ar9170	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic/initrd	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic/kernel	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic/kernel/arch	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic/kernel/fs	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic/kernel/fs/9p	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic/kernel/lib	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic/kernel/net	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic/kernel/sound	readdir	0xffffffffa02bd020
/lib/modules/2.6.38-8-generic/misc	readdir	0xffffffffa02bd020
/lib/security	readdir	0xffffffffa02bd020
/lib/x86_64-linux-gnu	readdir	0xffffffffa02bd020
/lib/x86_64-linux-gnu/security	readdir	0xffffffffa02bd020
/media	readdir	0xffffffffa02bd020
/media/malware	readdir	0xffffffffa02bd020
/opt	readdir	0xffffffffa02bd020
/opt/VBoxGuestAdditi.../VBoxGuestAdditions	readdir	0xffffffffa02bd020
/opt/VBoxGuestAdditions-4.1.8	readdir	0xffffffffa02bd020
/opt/VBoxGuestAdditions-4.1.8/bin	readdir	0xffffffffa02bd020
/opt/VBoxGuestAdditions-4.1.8/lib	readdir	0xffffffffa02bd020
/opt/VBoxGuestAdditions-4.1.8/sbin	readdir	0xffffffffa02bd020
/proc	readdir	0xffffffffa02bd000
/proc	readdir	0xffffffffa02bd020
/root	readdir	0xffffffffa02bd020
/root/.cache	readdir	0xffffffffa02bd020
/root/.config	readdir	0xffffffffa02bd020
/root/.dbus	readdir	0xffffffffa02bd020
/root/.pulse	readdir	0xffffffffa02bd020
/root/usr	readdir	0xffffffffa02bd020
/sbin	readdir	0xffffffffa02bd020
/selinux	readdir	0xffffffffa02bd020
/sys	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/tmp	readdir	0xffffffffa02bd020
/tmp/.esd-1000	readdir	0xffffffffa02bd020
/tmp/.ICE-unix	readdir	0xffffffffa02bd020
/tmp/.X11-unix	readdir	0xffffffffa02bd020
/tmp/keyring-nLdrWW	readdir	0xffffffffa02bd020
/tmp/orbit-richard	readdir	0xffffffffa02bd020
/tmp/pulse-Oq95HwknZJva	readdir	0xffffffffa02bd020
/tmp/ssh-hvKvcPmB1252	readdir	0xffffffffa02bd020
/usr	readdir	0xffffffffa02bd020
/usr/bin	readdir	0xffffffffa02bd020
/usr/lib	readdir	0xffffffffa02bd020
/usr/lib/bamf	readdir	0xffffffffa02bd020
/usr/lib/compiz	readdir	0xffffffffa02bd020
/usr/lib/compizconfig	readdir	0xffffffffa02bd020
/usr/lib/compizconfig/backends	readdir	0xffffffffa02bd020
/usr/lib/d-conf	readdir	0xffffffffa02bd020
/usr/lib/dri	readdir	0xffffffffa02bd020
/usr/lib/evolution	readdir	0xffffffffa02bd020
/usr/lib/evolution/2.32	readdir	0xffffffffa02bd020
/usr/lib/gdk-pixbuf-2.0	readdir	0xffffffffa02bd020
/usr/lib/gdk-pixbuf-2.0/2.10.0	readdir	0xffffffffa02bd020
/usr/lib/gdk-pixbuf-2.0/2.10.0/loaders	readdir	0xffffffffa02bd020
/usr/lib/gdm	readdir	0xffffffffa02bd020
/usr/lib/geoclue	readdir	0xffffffffa02bd020
/usr/lib/gio	readdir	0xffffffffa02bd020
/usr/lib/gio/modules	readdir	0xffffffffa02bd020
/usr/lib/gnome-disk-utility	readdir	0xffffffffa02bd020
/usr/lib/gnome-settings-daemon	readdir	0xffffffffa02bd020
/usr/lib/gnome-settings-daemon-2.0	readdir	0xffffffffa02bd020
/usr/lib/gtk-2.0	readdir	0xffffffffa02bd020
/usr/lib/gtk-2.0/2.10.0	readdir	0xffffffffa02bd020
/usr/lib/gtk-2.0/2.10.0/engines	readdir	0xffffffffa02bd020
/usr/lib/gtk-2.0/2.10.0/immodules	readdir	0xffffffffa02bd020
/usr/lib/gtk-2.0/2.10.0/menuproxies	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/usr/lib/gtk-2.0/modules	readdir	0xffffffffa02bd020
/usr/lib/gvfs	readdir	0xffffffffa02bd020
/usr/lib/indicator-application	readdir	0xffffffffa02bd020
/usr/lib/indicator-datetime	readdir	0xffffffffa02bd020
/usr/lib/indicator-me	readdir	0xffffffffa02bd020
/usr/lib/indicator-messages	readdir	0xffffffffa02bd020
/usr/lib/indicators	readdir	0xffffffffa02bd020
/usr/lib/indicators/5	readdir	0xffffffffa02bd020
/usr/lib/indicator-session	readdir	0xffffffffa02bd020
/usr/lib/indicator-sound	readdir	0xffffffffa02bd020
/usr/lib/libgconf2-4	readdir	0xffffffffa02bd020
/usr/lib/libgconf2-4/2	readdir	0xffffffffa02bd020
/usr/lib/libvte9	readdir	0xffffffffa02bd020
/usr/lib/locale	readdir	0xffffffffa02bd020
/usr/lib/mesa	readdir	0xffffffffa02bd020
/usr/lib/ModemManager	readdir	0xffffffffa02bd020
/usr/lib/nautilus	readdir	0xffffffffa02bd020
/usr/lib/nautilus/extensions-2.0	readdir	0xffffffffa02bd020
/usr/lib/NetworkManager	readdir	0xffffffffa02bd020
/usr/lib/notify-osd	readdir	0xffffffffa02bd020
/usr/lib/policykit-1	readdir	0xffffffffa02bd020
/usr/lib/policykit-1-gnome	readdir	0xffffffffa02bd020
/usr/lib/pulse-0.9.22	readdir	0xffffffffa02bd020
/usr/lib/pulse-0.9.22/modules	readdir	0xffffffffa02bd020
/usr/lib/pulseaudio	readdir	0xffffffffa02bd020
/usr/lib/pulseaudio/pulse	readdir	0xffffffffa02bd020
/usr/lib/pyshared	readdir	0xffffffffa02bd020
/usr/lib/pyshared/py....7/gtk-2.0/pynotify	readdir	0xffffffffa02bd020
/usr/lib/pyshared/python2.7	readdir	0xffffffffa02bd020
/usr/lib/pyshared/python2.7/cairo	readdir	0xffffffffa02bd020
/usr/lib/pyshared/python2.7/gtk-2.0	readdir	0xffffffffa02bd020
/usr/lib/pyshared/python2.7/gtk-2.0/gtk	readdir	0xffffffffa02bd020
/usr/lib/python2.7	readdir	0xffffffffa02bd020
/usr/lib/python2.7/d...ackages/gtk-2.0/gio	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/usr/lib/python2.7/dist-packages	readdir	0xffffffffa02bd020
/usr/lib/python2.7/dist-packages/glib	readdir	0xffffffffa02bd020
/usr/lib/python2.7/dist-packages/gobject	readdir	0xffffffffa02bd020
/usr/lib/python2.7/dist-packages/gtk-2.0	readdir	0xffffffffa02bd020
/usr/lib/python2.7/dist-packages/xapian	readdir	0xffffffffa02bd020
/usr/lib/python2.7/lib-dynload	readdir	0xffffffffa02bd020
/usr/lib/rsyslog	readdir	0xffffffffa02bd020
/usr/lib/rtkit	readdir	0xffffffffa02bd020
/usr/lib/udisks	readdir	0xffffffffa02bd020
/usr/lib/unity	readdir	0xffffffffa02bd020
/usr/lib/unity-place-applications	readdir	0xffffffffa02bd020
/usr/lib/unity-place-files	readdir	0xffffffffa02bd020
/usr/lib/upower	readdir	0xffffffffa02bd020
/usr/lib/x86_64-linu...pango/1.6.0/modules	readdir	0xffffffffa02bd020
/usr/lib/x86_64-linux-gnu	readdir	0xffffffffa02bd020
/usr/lib/x86_64-linux-gnu/gconv	readdir	0xffffffffa02bd020
/usr/lib/x86_64-linux-gnu/pango	readdir	0xffffffffa02bd020
/usr/lib/x86_64-linux-gnu/pango/1.6.0	readdir	0xffffffffa02bd020
/usr/lib/xorg	readdir	0xffffffffa02bd020
/usr/lib/xorg/modules	readdir	0xffffffffa02bd020
/usr/lib/xorg/modules/extensions	readdir	0xffffffffa02bd020
/usr/lib/xorg/modules/input	readdir	0xffffffffa02bd020
/usr/local	readdir	0xffffffffa02bd020
/usr/local/bin	readdir	0xffffffffa02bd020
/usr/local/sbin	readdir	0xffffffffa02bd020
/usr/local/share	readdir	0xffffffffa02bd020
/usr/sbin	readdir	0xffffffffa02bd020
/usr/share	readdir	0xffffffffa02bd020
/usr/share/applications	readdir	0xffffffffa02bd020
/usr/share/fonts	readdir	0xffffffffa02bd020
/usr/share/fonts/tru.../ubuntu-font-family	readdir	0xffffffffa02bd020
/usr/share/fonts/truetype	readdir	0xffffffffa02bd020
/usr/share/fonts/truetype/ttf-dejavu	readdir	0xffffffffa02bd020
/usr/share/glib-2.0	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/usr/share/glib-2.0/schemas	readdir	0xffffffffa02bd020
/usr/share/icons	readdir	0xffffffffa02bd020
/usr/share/icons/DMZ-White	readdir	0xffffffffa02bd020
/usr/share/icons/DMZ-White/cursors	readdir	0xffffffffa02bd020
/usr/share/icons/gnome	readdir	0xffffffffa02bd020
/usr/share/icons/hicolor	readdir	0xffffffffa02bd020
/usr/share/icons/Humanity	readdir	0xffffffffa02bd020
/usr/share/icons/Humanity-Dark	readdir	0xffffffffa02bd020
/usr/share/icons/ubuntu-mono-dark	readdir	0xffffffffa02bd020
/usr/share/icons/unity-icon-theme	readdir	0xffffffffa02bd020
/usr/share/locale	readdir	0xffffffffa02bd020
/usr/share/locale/en	readdir	0xffffffffa02bd020
/usr/share/locale/en/LC_MESSAGES	readdir	0xffffffffa02bd020
/usr/share/locale-la...k/en_US/LC_MESSAGES	readdir	0xffffffffa02bd020
/usr/share/locale-langpack	readdir	0xffffffffa02bd020
/usr/share/locale-langpack/en	readdir	0xffffffffa02bd020
/usr/share/locale-langpack/en/LC_MESSAGES	readdir	0xffffffffa02bd020
/usr/share/locale-langpack/en_US	readdir	0xffffffffa02bd020
/usr/share/mime	readdir	0xffffffffa02bd020
/usr/share/vte	readdir	0xffffffffa02bd020
/usr/share/vte/termcap-0.0	readdir	0xffffffffa02bd020
/usr/share/zoneinfo	readdir	0xffffffffa02bd020
/usr/share/zoneinfo/Africa	readdir	0xffffffffa02bd020
/var	readdir	0xffffffffa02bd020
/var/cache	readdir	0xffffffffa02bd020
/var/cache/fontconfig	readdir	0xffffffffa02bd020
/var/cache/software-center	readdir	0xffffffffa02bd020
/var/cache/software-center/xapian	readdir	0xffffffffa02bd020
/var/lib	readdir	0xffffffffa02bd020
/var/lib/dhcp	readdir	0xffffffffa02bd020
/var/lib/NetworkManager	readdir	0xffffffffa02bd020
/var/lock	readdir	0xffffffffa02bd020
/var/log	readdir	0xffffffffa02bd020
/var/log/ConsoleKit	readdir	0xffffffffa02bd020

Symbol Name	Member	Address
/var/log/gdm	readdir	0xffffffffa02bd020
/var/mail	readdir	0xffffffffa02bd020
/var/run	readdir	0xffffffffa02bd020
/var/spool	readdir	0xffffffffa02bd020
/var/spool/anacron	readdir	0xffffffffa02bd020
/var/spool/cron	readdir	0xffffffffa02bd020
/var/spool/cron/atjobs	readdir	0xffffffffa02bd020
/var/spool/cron/crontabs	readdir	0xffffffffa02bd020
anacron 3 []	readdir	0xffffffffa02bd020
proc_mnt: root	readdir	0xffffffffa02bd000
proc_root	readdir	0xffffffffa02bd000

This page intentionally left blank.

Bibliography

Carbone, R. File recovery and data extraction using automated data recovery tools: A balanced approach using Windows and Linux when working with an unknown disk image and filesystem. TM 2009-161. Technical memorandum. Defence R&D Canada – Valcartier. January 2013.

Carbone, R. Malware memory analysis for non-specialists: Investigating a publicly available memory image of the Zeus Trojan horse. TM 2013-018. Technical memorandum. Defence R&D Canada – Valcartier. April 2013.

Carbone, R. Malware memory analysis for non-specialists: Investigating publicly available memory images for Prolaco and SpyEye. TM 2013-155. Technical memorandum. Defence R&D Canada – Valcartier. October 2013.

Carbone, R. Malware memory analysis for non-specialists: Investigating publicly available memory image 0zapftis (R2D2). TM 2013-177. Technical memorandum. Defence R&D Canada – Valcartier. October 2013.

Carbone, R. Malware memory analysis for non-specialists: Investigating publicly available memory image for the Stuxnet worm. SR DRDC-RDDC-2013-R1. Scientific report. Defence R&D Canada – Valcartier. November 2013.

Carbone, R. Malware memory analysis for non-specialists: Investigating publicly available memory image for the Tigger Trojan horse. SR DRDC-RDDC-2014-R28. Scientific report. Defence R&D Canada – Valcartier. June 2014.

Carbone, Richard. Malware memory analysis of the KBeast rootkit: Investigating publicly available Linux rootkits using the Volatility memory analysis framework. Scientific Report (in preparation for publishing). Defence R&D Canada – Valcartier. September 2014.

Hale Ligh, Michael; Case, Andrew et al. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Max Memory. Book. John Wiley & Sons. July 2014.

List of symbols/abbreviations/acronyms/initialisms

API	Application Programming Interface
AV	Anti-virus or antivirus
BIOS	Basic Input/Output System
CAF	Canadian Armed Forces
CFNOC	Canadian Forces Network Operation Centre
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service / Domain Name Server
DRDC	Defence Research and Development Canada
DSL	Digital Subscriber Line
DTB	Directory Table Base
DVD	Digital Video Disc or Digital Versatile Disc
DVD +/- RW	Digital Video Disc +/- Read/Write
ECL	Export Control List
ELF	Executable and Linkable Format
eSATA	External SATA
EVT	Exception Vector Table
FAC	Forces armées canadiennes
GB	Gigabyte ($1x10^9$)
GCC	GNU C Compiler
GDDR5	Graphics Double Data Rate 5
GHz	Gigahertz
GiB	Gibibyte (2^{30} bytes)
GID	Group ID
ID	Identification
IDT	Interrupt Descriptor Table
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IT	Information Technology

ITCU	Integrated Technological Crime Unit
KiB	Kibibyte (2^{10} bytes)
LKM	Loadable Kernel Module
Lsof	LiSt Open Files
LTO5	Linear Tape Open 5
MD5	Message-Digest Algorithm 5
NAT	Network Address Translation
NSRL	National Software Reference Library
PAE	Physical Address Extension
PAM	Pluggable Authentication Module
PC	Personal Computer
PCI	Peripheral Component Interconnect
PID	Process ID
PO Box	Post-Office Box or Post Office Box
PPID	Parent Process ID
R&D	Research & Development
RAM	Random Access Memory
RCMP	Royal Canadian Mounted Police
SAS	Serial Attached SCSI
SATA	Serial ATA or Serial AT Attachment or
SHA1	Secure Hash Algorithm-1
SMP	Symmetric Multiprocessing
Syscall	System Call
TB	Terabyte ($1x10^{12}$)
TCP	Transmission Control Protocol
TCP	Transmission Control Protocol
TI	Technologie de l'information
TM	Technical Memorandum
TTY	TeleTYpe
UDP	User Datagram Protocol
UID	User ID

USB2/3	Universal Serial Bus 2/3
UTC	Coordinated Universal Time
VM	Virtual Machine
x64	64-bit PC architecture
x86	32-bit PC architecture

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Valcartier Research Centre
Defence Research and Development Canada
2459 route de la Bravoure
Québec (Québec) G3J 1X5
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2012

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Malware memory analysis of the IVYL Linux rootkit : Investigating a publicly available Linux rootkit using the Volatility memory analysis framework

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Carbone, R.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
April 2015	128	13

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientific Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Valcartier Research Centre
Defence Research and Development Canada
2459 route de la Bravoure
Québec (Québec) G3J 1X5
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2015-R060	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This report is the second in a series that will examine Linux Volatility-specific memory malware-based analysis techniques. Windows-based malware memory analysis techniques were analysed in a previous series. Unlike these Windows-based reports, some of the techniques described therein are not applicable to Linux-based analyses including data carving and anti-virus scanning. Thus, with minimal use of scanner-based technologies, the author will demonstrate what to look for while conducting Linux-specific Volatility-based investigations. Each investigation consists of an infected memory image and its accompanying Volatility memory profile that will be used to examine a different open source rootkit. Some of the rootkits are user-land while others are kernel-based. Rootkits were chosen over Trojans, worms and viruses as rootkits tend to be more sophisticated. This specific investigation examines the IVYL rootkit. It is hoped that through the proper application of various Volatility plugins combined with an in-depth knowledge of the Linux operating system, these case studies will provide guidance to other investigators in their own analyses.

Ce rapport est le second d'une série examinant les techniques spécifiques d'analyse de logiciels malveillants en mémoire sous Linux à l'aide de l'outil Volatility. Les techniques d'analyse de logiciels malveillants en mémoire pour Windows ont été décrites dans des rapports précédents. Cependant, certaines de ces techniques, telles que la récupération de données et le balayage d'antivirus ne s'appliquent pas aux analyses sous Linux. Par conséquent, avec une utilisation minimale des technologies de balayage, l'auteur démontrera ce qu'il faut rechercher lorsqu'on effectue des investigations spécifiques à Linux avec Volatility. Chaque investigation consiste en une image mémoire infectée, accompagnée de son profile mémoire Volatility, et examinera un programme malveillant furtif à code source ouvert différent. Certains seront en mode utilisateur tandis que d'autres seront en mode noyau. Les programmes malveillants furtifs ont été préférés aux chevaux de Troie, vers et virus, car ils ont tendance à être plus sophistiqués. La présente investigation examine spécifiquement le programme malveillant furtif IVYL. Il est espéré qu'avec une utilisation adéquate de différents plugiciels Volatility et d'une connaissance approfondie du système d'exploitation Linux, ces études de cas fourniront des conseils à d'autres enquêteurs pour leurs propres analyses.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Anti-virus; Antivirus; Computer forensics; Computer infection; Computer memory forensics; Digital forensics; Digital memory forensics; Forensics; Infection; IVYL; Linux; Malware; Memory analysis; Memory forensics; Memory image; Rootkit; Scanners; Virus scanner; Volatility